



## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2002041482 A**(43) Date of publication of application: **08.02.02**

(51) Int. Cl. **G06F 15/00**  
**G09C 1/00**  
**H04L 9/08**  
**H04L 9/10**  
**H04L 9/32**  
**H04N 5/85**  
**H04N 5/91**  
**H04N 7/167**

(21) Application number: **2000220720**(22) Date of filing: **21.07.00**(71) Applicant: **HITACHI LTD SEGA CORP**

(72) Inventor:  
**NISHIOKA GENJI**  
**SETO YOICHI**  
**WAKABAYASHI TAKASHI**  
**TETSUI TOSHIAKI**  
**YAMANAKA ISATAKE**

(54) **METHOD FOR RELEASING CONTENTS  
 UTILIZATION LIMITATION AND STORAGE  
 MEDIUM**

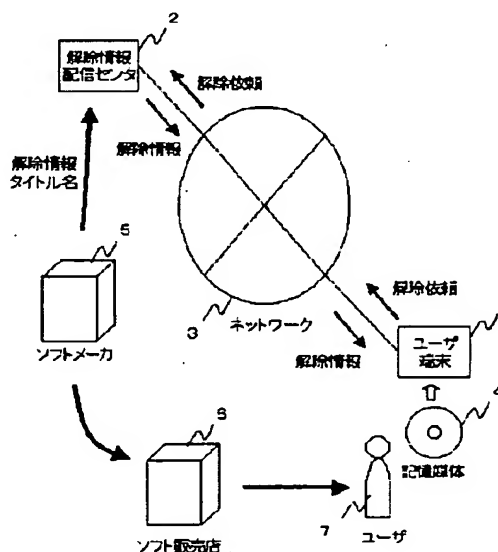
## (57) Abstract:

**PROBLEM TO BE SOLVED:** To evaluate contents in advance of the formal purchase of the contents, without imposing excessive load on a user.

**SOLUTION:** The contents the utilization of a part of which is limited by some method are stored together with a utilization limitation release program in a storage medium 4 and offered to the user. The user inserts the purchased storage medium 4 into a user terminal 1 and can actually try available part of the contents. When the user likes the part, the user starts the utilization limitation release program, transmits a release request which includes the title name of the contents to a release information distribution center 2 via a network 3 and can purchase the release information of the contents. The utilization limitation of the contents can be released by the utilization limitation release program.

COPYRIGHT: (C)2002,JPO

図1



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-41482

(P2002-41482A)

(43) 公開日 平成14年2月8日(2002.2.8)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テームコード <sup>8</sup> (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 Z 5 B 0 8 5
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 A 5 C 0 5 2
H 0 4 L 9/08		H 0 4 N 5/85	Z 5 C 0 5 3
9/10		H 0 4 L 9/00	6 0 1 A 5 C 0 6 4
9/32			6 0 1 E 5 J 1 0 4

審査請求 未請求 請求項の数21 O L (全 30 頁) 最終頁に続く

(21) 出願番号 特願2000-220720(P2000-220720)

(22) 出願日 平成12年7月21日(2000.7.21)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(71) 出願人 000132471

株式会社セガ

東京都大田区羽田1丁目2番12号

(72) 発明者 西岡 玄次

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(74) 代理人 100087170

弁理士 富田 和子

最終頁に続く

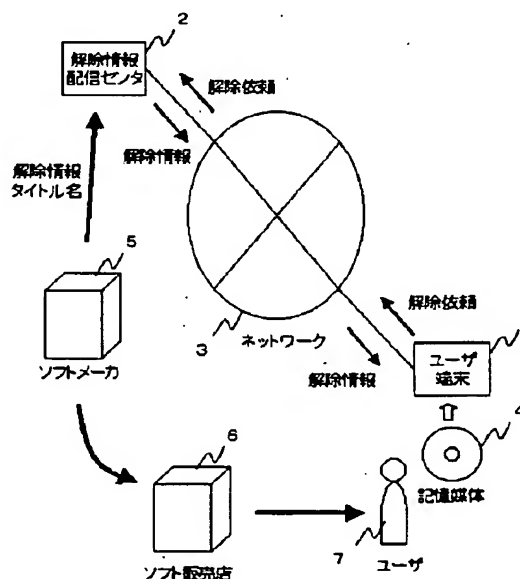
(54) 【発明の名称】 コンテンツの利用制限解除方法および記憶媒体

(57) 【要約】

【課題】 ユーザに過度の負担をかけることなく、コンテンツの正規購入に先だってそのコンテンツを評価できるようにする。

【解決手段】 一部の部分の利用を何らかの方法により制限したコンテンツを利用制限解除プログラムと共に記憶媒体4に格納してユーザに提供する。ユーザは、購入した記憶媒体4をユーザ端末1に装着し、コンテンツの利用可能な部分を実際に試すことができる。気に入った場合には、利用制限解除プログラムを起動させ、ネットワーク3を介して解除情報配信センタ2に前記コンテンツのタイトル名を含む解除依頼を送信し、当該コンテンツの解除情報を購入できる。そして、この利用制限解除プログラムによりコンテンツの利用制限を解除できる。

図1



## 【特許請求の範囲】

【請求項1】コンテンツを、一部を利用可能とし、その他の部分の利用を制限して、当該コンテンツの利用制限を解除するためのプログラムと共に記憶媒体に格納し、配布するステップと、

サーバが、ネットワークを介して、前記記憶媒体が装着された端末から解除依頼を受け付けると、当該記憶媒体に前記コンテンツと共に格納されている前記プログラムが当該コンテンツの利用制限を解除するのに使用する解除情報を、前記端末に送信するステップと、を有することを特徴とするコンテンツの利用制限解除方法。

【請求項2】記憶媒体が装着された端末にネットワークを介して接続されたサーバを用いて、当該記憶媒体に記憶されている、一部が利用可能であり、その他の部分の利用が制限されたコンテンツの利用制限を解除する、コンテンツの利用制限解除方法であって、

前記端末において、前記コンテンツの利用制限の解除依頼を前記サーバに送信する解除依頼ステップと、

前記サーバにおいて、前記端末より受信した解除依頼にしたがい、前記コンテンツの利用制限を解除するための解除情報を、当該コンテンツに固有の鍵を用いた暗号通信により前記端末と共有した鍵で暗号化し、前記端末に送信する解除情報送信ステップと、

前記端末において、前記サーバより受信した暗号文を、前記記憶媒体に記憶されている前記コンテンツに固有の鍵を用いた暗号通信により、前記サーバと共有した鍵で復号化し、その結果得られた解除情報を用いて、前記コンテンツの利用制限を解除する利用制限解除ステップと、を有することを特徴とするコンテンツの利用制限解除方法。

【請求項3】請求項2記載のコンテンツの利用制限解除方法であって、

前記コンテンツは、前記その他の部分が暗号化されて、その利用が制限されたものであり、且つ、前記記憶媒体には、前記コンテンツと共に、共通鍵暗号体系に従った当該コンテンツに固有の鍵情報 $GK$ が記憶されており、前記解除依頼ステップは、

乱数を用いて鍵 $K_1$ を生成し、当該鍵 $K_1$ と当該端末のユーザ情報 $ID_1$ とを含む情報を、前記記憶媒体から読み出した鍵情報 $GK$ を用いて暗号化し、その暗号結果である暗号文 $C_{1,1}$ と前記ユーザ情報 $ID_1$ とを、解除依頼として、前記サーバに送信するものであり、

前記解除情報送信ステップは、

予め用意してある前記コンテンツに固有の鍵情報 $GK$ を用いて、前記端末より受信した暗号文 $C_{1,1}$ を復号化し、その結果得られたユーザ情報 $ID_1$ と、前記暗号文 $C_{1,1}$ と共に送られてきたユーザ情報 $ID_1$ とを用いてユーザ認証を行うサーバ側ユーザ認証ステップと、

前記サーバ側ユーザ認証ステップでのユーザ認証が成立した場合に、前記コンテンツの暗号化部分を復号化する

ための復号鍵 $K$ （解除情報）と前記ユーザ情報 $ID_1$ とを含む情報を、前記暗号文 $C_{1,1}$ を復号化した結果得られた鍵 $K_1$ を用いて暗号化し、その暗号結果である暗号文 $C_{1,2}$ を、前記端末に送信する鍵送信ステップと、を有し、

前記利用制限解除ステップは、

前記解除依頼ステップで生成した暗号文 $C_{1,1}$ を前記記憶媒体から読み出した鍵情報 $GK$ を用いて復号化し、次いで、その結果得られた鍵 $K_1$ を用いて、前記サーバから受信した暗号文 $C_{1,2}$ を復号化し、その結果得られたユーザ情報 $ID_1$ を用いて、ユーザ認証を行う端末側ユーザ認証ステップと、

前記端末側ユーザ認証ステップでのユーザ認証が成立した場合に、前記暗号文 $C_{1,2}$ を復号化した結果得られた復号鍵 $K$ を用いて、前記コンテンツの暗号化部分を復号化するコンテンツ復号化ステップと、を有することを特徴とするコンテンツの利用制限解除方法。

【請求項4】請求項3記載のコンテンツの利用制限解除方法であって、

前記鍵送信ステップは、

前記サーバ側ユーザ認証ステップでのユーザ認証が成立した場合に、乱数 $R$ を生成し、当該乱数 $R$ と前記復号鍵 $K$ と前記ユーザ情報 $ID_1$ とを、前記暗号文 $C_{1,1}$ を復号化した結果得られた鍵 $K_1$ を用いて暗号化し、その暗号結果である暗号文 $C_{1,2}$ を、前記端末に送信することを特徴とするコンテンツの利用制限解除方法。

【請求項5】請求項2記載のコンテンツの利用制限解除方法であって、

前記コンテンツは、前記その他の部分が暗号化されて、その利用が制限されたものであり、且つ、前記記憶媒体には、前記コンテンツと共に、共通鍵暗号体系に従った当該コンテンツに固有の鍵情報 $GK_1$ 、 $GK_2$ が記憶されており、

前記解除依頼ステップは、

乱数を用いて鍵 $K_{1,1}$ 、 $K_{1,2}$ を生成し、前記鍵 $K_{1,2}$ を前記記憶媒体から読み出した鍵情報 $GK_2$ を用いて暗号化し、次いで、その暗号結果である暗号文 $C_{1,1}$ と前記鍵 $K_{1,1}$ と当該端末のユーザ情報 $ID_1$ とを、前記記憶媒体から読み出した鍵情報 $GK_1$ を用いて暗号化し、その暗号結果である暗号文 $C_{1,1}$ と前記ユーザ情報 $ID_1$ とを、解除依頼として、前記サーバに送信するものであり、

前記解除情報送信ステップは、

予め用意してある前記コンテンツに固有の鍵情報 $GK_2$ を用いて、前記端末から受信した暗号文 $C_{1,1}$ を復号化し、その結果得られたユーザ情報 $ID_1$ と、前記暗号文 $C_{1,1}$ と共に送られてきたユーザ情報 $ID_1$ とを用いてユーザ認証を行うサーバ側ユーザ認証ステップと、

前記サーバ側ユーザ認証ステップでのユーザ認証が成立した場合に、予め用意してある前記コンテンツに固有の鍵情報 $GK_1$ を用いて、前記暗号文 $C_{1,1}$ を復号化した結果

得られた暗号文 $C_{i,j}$ を復号化し、その結果得られた鍵 $K_{i,j}$ を用いて前記コンテンツの暗号化部分を復号化するための復号鍵 $K$ (解除情報)を暗号化し、次いで、その暗号結果である暗号文 $C_{i,j}$ と前記ユーザ情報 $ID_i$ とを、前記暗号文 $C_{i,j}$ を復号化した結果得られた鍵 $K_{i,j}$ を用いて暗号化し、その結果得られた暗号文 $C_{i,j}$ を、前記端末に送信する鍵送信ステップと、を有し、

前記利用制限解除ステップは、

前記解除情報依頼送信ステップで生成した暗号文 $C_{i,j}$ を前記記憶媒体から読み出した鍵情報 $GK_i$ を用いて復号化し、次いで、その結果得られた鍵 $K_{i,j}$ を用いて前記サーバから受信した暗号文 $C_{i,j}$ を復号化し、その結果得られたユーザ情報 $ID_i$ を用いて、ユーザ認証を行う端末側ユーザ認証ステップと、

前記端末側ユーザ認証ステップでのユーザ認証が成立した場合に、前記暗号文 $C_{i,j}$ を復号化した結果得られた暗号文 $C_{i,j}$ を前記記憶媒体から読み出した鍵情報 $GK_i$ を用いて復号化し、その結果得られた鍵 $K_{i,j}$ を用いて、前記暗号文 $C_{i,j}$ を復号化した結果得られた暗号文 $C_{i,j}$ を復号化して、復号鍵 $K$ を入手し、当該復号鍵 $K$ を用いて前記コンテンツの暗号化部分を復号化するコンテンツ復号化ステップと、を有することを特徴とするコンテンツの利用制限解除方法。

【請求項6】請求項2記載のコンテンツの利用制限解除方法であって、

前記記憶媒体には、前記コンテンツと共に、共通鍵暗号体系に従った当該コンテンツに固有の鍵情報 $GK$ と、当該コンテンツに固有の認証情報 $AK$ とが記憶されており、前記解除依頼ステップは、

乱数を用いて鍵 $K_i$ を生成し、当該鍵 $K_i$ と当該端末のユーザ情報 $ID_i$ とを含む情報を、前記記憶媒体から読み出した鍵情報 $GK$ を用いて暗号化し、その暗号結果である暗号文 $C_{i,j}$ と前記ユーザ情報 $ID_i$ とを、解除依頼として、前記サーバに送信するものであり、

前記解除情報送信ステップは、

予め用意してある前記コンテンツに固有の鍵情報 $GK$ を用いて、前記端末より受信した暗号文 $C_{i,j}$ を復号化し、その結果得られたユーザ情報 $ID_i$ と、前記暗号文 $C_{i,j}$ と共に送られてきたユーザ情報 $ID_i$ とを用いてユーザ認証を行うサーバ側ユーザ認証ステップと、

前記サーバ側ユーザ認証ステップでのユーザ認証が成立した場合に、前記コンテンツの利用制限を解除するための認証情報 $AK$ (解除情報)と前記ユーザ情報 $ID_i$ とを含む情報を、前記暗号文 $C_{i,j}$ を復号化した結果得られた鍵 $K_{i,j}$ を用いて暗号化し、その暗号結果である暗号文 $C_{i,j}$ を、前記端末に送信する認証情報送信ステップと、を有し、

前記利用制限解除ステップは、

前記解除依頼ステップで生成した暗号文 $C_{i,j}$ を前記記憶媒体から読み出した鍵情報 $GK$ を用いて復号化し、次い

で、その結果得られた鍵 $K_{i,j}$ を用いて、前記サーバから受信した暗号文 $C_{i,j}$ を復号化し、その結果得られたユーザ情報 $ID_i$ を用いて、ユーザ認証を行う端末側ユーザ認証ステップと、

前記端末側ユーザ認証ステップでのユーザ認証が成立した場合に、前記暗号文 $C_{i,j}$ を復号化した結果得られた認証情報 $AK$ と、前記記憶媒体に記憶されている認証情報 $AK$ とを比較して、両者が一致する場合に、前記コンテンツの利用が制限されている部分へのアクセスを許可するアクセス許可ステップと、を有することを特徴とするコンテンツの利用制限解除方法。

【請求項7】請求項6記載のコンテンツの利用制限解除方法であって、

前記認証情報送信ステップは、

前記サーバ側ユーザ認証ステップでのユーザ認証が成立した場合に、乱数 $R$ を生成し、当該乱数 $R$ と前記認証情報 $AK$ と前記ユーザ情報 $ID_i$ とを、前記暗号文 $C_{i,j}$ を復号化した結果得られた鍵 $K_{i,j}$ を用いて暗号化し、その暗号結果である暗号文 $C_{i,j}$ を、前記端末に送信することを特徴とするコンテンツの利用制限解除方法。

【請求項8】請求項2記載のコンテンツの利用制限解除方法であって、

前記記憶媒体には、前記コンテンツと共に、共通鍵暗号体系に従った当該コンテンツに固有の鍵情報 $GK_i$ 、 $GK_j$ と、当該コンテンツに固有の認証情報 $AK$ とが記憶されており、

前記解除依頼ステップは、

乱数を用いて鍵 $K_{i,j}$ 、 $K_{j,i}$ を生成し、前記鍵 $K_{i,j}$ を前記記憶媒体から読み出した鍵情報 $GK_i$ を用いて暗号化し、次いで、その暗号結果である暗号文 $C_{i,j}$ と前記鍵 $K_{j,i}$ と当該端末のユーザ情報 $ID_i$ とを、前記記憶媒体から読み出した鍵情報 $GK_j$ を用いて暗号化し、その暗号結果である暗号文 $C_{i,j}$ と前記ユーザ情報 $ID_i$ とを、解除依頼として、前記サーバに送信するものであり、

前記解除情報送信ステップは、

予め用意してある前記コンテンツに固有の鍵情報 $GK_i$ を用いて、前記端末から受信した暗号文 $C_{i,j}$ を復号化し、その結果得られたユーザ情報 $ID_i$ と、前記暗号文 $C_{i,j}$ と共に送られてきたユーザ情報 $ID_i$ とを用いてユーザ認証を行うサーバ側ユーザ認証ステップと、

前記サーバ側ユーザ認証ステップでのユーザ認証が成立した場合に、予め用意してある前記コンテンツに固有の鍵情報 $GK_j$ を用いて、前記暗号文 $C_{i,j}$ を復号化した結果得られた暗号文 $C_{i,j}$ を復号化し、その結果得られた鍵 $K_{i,j}$ を用いて前記コンテンツの利用制限を解除するための認証情報 $AK$ (解除情報)を暗号化し、次いで、その暗号結果である暗号文 $C_{i,j}$ と前記ユーザ情報 $ID_i$ とを、前記暗号文 $C_{i,j}$ を復号化した結果得られた鍵 $K_{i,j}$ を用いて暗号化し、その結果得られた暗号文 $C_{i,j}$ を、前記端末に送信する認証情報送信ステップと、を有し、

5

前記利用制限解除ステップは、  
前記解除依頼ステップで生成した暗号文 $C_{i,j}$ を前記記憶媒体から読み出した鍵情報 $K_k$ を用いて復号化し、次いで、その結果得られた鍵 $K_{k_1}$ を用いて前記サーバから受信した暗号文 $C_{i,j}$ を復号化し、その結果得られたユーザ情報 $ID_k$ を用いて、ユーザ認証を行う端末側ユーザ認証ステップと、  
前記端末側ユーザ認証ステップでのユーザ認証が成立した場合に、前記暗号文 $C_{i,j}$ を復号化した結果得られた暗号文 $C_{i,j}$ を前記記憶媒体から読み出した鍵情報 $K_k$ を用いて復号化し、その結果得られた鍵 $K_{k_2}$ を用いて、前記暗号文 $C_{i,j}$ を復号化した結果得られた暗号文 $C_{i,j}$ を復号化して、認証情報 $AK$ を入手し、当該認証情報 $AK$ と前記記憶媒体に記憶されている認証情報 $AK$ とを比較して、両者が一致する場合に、前記コンテンツの利用が制限されている部分へのアクセスを許可するアクセス許可ステップと、を有することを特徴とするコンテンツの利用制限解除方法。

【請求項9】記憶媒体が装着された端末にネットワークを介して接続されたサーバを用いて、当該記憶媒体に記憶されている、一部が利用可能であり、その他の部分の利用が制限されたコンテンツの利用制限を解除する、コンテンツの利用制限解除方法であって、  
前記端末において、前記コンテンツの利用制限の解除依頼を前記サーバに送信する解除依頼ステップと、  
前記サーバにおいて、前記端末から受信した解除依頼にしたがい、前記コンテンツの利用制限を解除するための解除情報を、当該コンテンツに固有の暗号鍵で暗号化し、前記端末に送信する解除情報送信ステップと、  
前記端末において、前記サーバより受信した暗号文を、前記記憶媒体に記憶されている、前記コンテンツに固有の暗号鍵と対の復号鍵であって前記暗号鍵を推測不可能な復号鍵で、復号化し、その結果得られた解除情報を用いて、前記コンテンツの利用制限を解除する利用制限解除ステップと、を有することを特徴とするコンテンツの利用制限解除方法。

【請求項10】請求項9記載のコンテンツの利用制限解除方法であって、  
前記コンテンツは、前記その他の部分が暗号化されて、その利用が制限されたものであり、且つ、前記記憶媒体には、前記コンテンツと共に、非対称鍵暗号体系に従った当該コンテンツに固有の鍵であって、当該鍵からは前記サーバが保持する当該鍵と対の暗号鍵 $K_k$ を推測不可能な復号鍵 $K_r$ が記憶されており、  
前記解除情報送信ステップは、  
前記端末より受信した解除依頼に含まれるユーザ情報 $ID_k$ を用いて、ユーザ認証を行うサーバ側ユーザ認証ステップと、  
前記サーバ側ユーザ認証ステップでのユーザ認証が成立した場合に、予め用意してある前記暗号鍵 $K_k$ を用いて、  
40 前記コンテンツの暗号化部分を復号化するための復号鍵 $K$ （解除情報）を暗号化し、次いで、その暗号結果である $C_{i,j}$ と前記端末より受信した解除依頼に含まれるユーザ情報 $ID_k$ とを、予め用意してある前記暗号鍵 $K_{k_1}$ を用いて暗号化し、その暗号結果である暗号文 $C_{i,j}$ を前記端末に送信する鍵送信ステップと、を有し、  
前記利用制限解除ステップは、  
前記サーバから受信した暗号文 $C_{i,j}$ を前記記憶媒体から読み出した前記復号鍵 $K_r$ を用いて復号化し、その結果得られたユーザ情報 $ID_k$ を用いて、ユーザ認証を行う端末側ユーザ認証ステップと、  
50 前記端末側認証ステップでのユーザ認証が成立した場合

6

前記端末より受信した解除依頼に含まれるユーザ情報 $ID_k$ と前記コンテンツの暗号化部分を復号化するための復号鍵 $K$ （解除情報）とを含む情報を暗号化し、その暗号結果である暗号文 $C_{i,j}$ を、前記端末に送信する鍵送信ステップと、を有し、

前記利用制限解除ステップは、  
前記サーバから受信した暗号文 $C_{i,j}$ を前記記憶媒体から読み出した前記復号鍵 $K_r$ を用いて復号化し、その結果得られたユーザ情報 $ID_k$ を用いて、ユーザ認証を行う端末側ユーザ認証ステップと、  
前記端末側ユーザ認証ステップでのユーザ認証が成立した場合に、前記暗号文 $C_{i,j}$ を復号化した結果得られた復号鍵 $K$ を用いて、前記コンテンツの暗号化部分を復号化するコンテンツ復号化ステップと、を有することを特徴とするコンテンツの利用制限解除方法。

【請求項11】請求項10記載のコンテンツの利用制限解除方法であって、

前記鍵送信ステップは、  
前記サーバ側ユーザ認証ステップでのユーザ認証が成立した場合に、乱数 $R$ を生成し、当該乱数 $R$ と前記復号鍵 $K$ と前記ユーザ情報 $ID_k$ とを、予め用意してある前記暗号鍵 $K_k$ を用いて暗号化し、その暗号結果である暗号文 $C_{i,j}$ を、前記端末に送信することを特徴とするコンテンツの利用制限解除方法。

【請求項12】請求項9記載のコンテンツの利用制限解除方法であって、

前記コンテンツは、前記その他の部分が暗号化されて、その利用が制限されたものであり、且つ、前記記憶媒体には、前記コンテンツと共に、非対称鍵暗号体系に従った当該コンテンツに固有の鍵であって、当該鍵からは、前記サーバが保持する当該鍵と対の暗号鍵 $K_{k_1}$ 、 $K_{k_2}$ を、推測不可能な復号鍵 $K_{r_1}$ 、 $K_{r_2}$ が記憶されており、

前記解除情報送信ステップは、  
前記端末より受信した解除依頼に含まれるユーザ情報 $ID_k$ を用いて、ユーザ認証を行うサーバ側ユーザ認証ステップと、

前記サーバ側ユーザ認証ステップでのユーザ認証が成立した場合に、予め用意してある前記暗号鍵 $K_{k_2}$ を用いて前記コンテンツの暗号化部分を復号化するための復号鍵 $K$ （解除情報）を暗号化し、次いで、その暗号結果である $C_{i,j}$ と前記端末より受信した解除依頼に含まれるユーザ情報 $ID_k$ とを、予め用意してある前記暗号鍵 $K_{k_1}$ を用いて暗号化し、その暗号結果である暗号文 $C_{i,j}$ を前記端末に送信する鍵送信ステップと、を有し、

前記利用制限解除ステップは、  
前記サーバから受信した暗号文 $C_{i,j}$ を前記記憶媒体から読み出した前記復号鍵 $K_{r_2}$ を用いて復号化し、その結果得られたユーザ情報 $ID_k$ を用いて、ユーザ認証を行う端末側ユーザ認証ステップと、  
前記端末側認証ステップでのユーザ認証が成立した場合

に、前記暗号文 $C_{i,j}$ を復号化した結果得られた暗号文 $C_{i,j}$ を、前記記憶媒体から読み出した前記復号鍵 $K_{i,j}$ を用いて復号化して、復号鍵 $K$ を入手し、当該復号鍵 $K$ を用いて、前記コンテンツの暗号化部分を復号化するコンテンツ復号化ステップと、を有することを特徴とするコンテンツの利用制限解除方法。

【請求項13】請求項9記載のコンテンツの利用制限解除方法であって、

前記記憶媒体には、前記コンテンツと共に、非対称鍵暗号体系に従った当該コンテンツに固有の鍵であって、当該鍵からは前記サーバが保持する当該鍵と対の暗号鍵 $K_i$ を推測不可能な復号鍵 $K_i$ と、当該コンテンツに固有の認証情報 $AK$ とが記憶されており、

前記解除情報送信ステップは、

前記端末より受信した解除依頼に含まれるユーザ情報 $ID$ を用いて、ユーザ認証を行うサーバ側ユーザ認証ステップと、

前記サーバ側ユーザ認証ステップでのユーザ認証が成立した場合に、予め用意してある前記暗号鍵 $K_i$ を用いて、前記端末より受信した解除依頼に含まれるユーザ情報 $ID$ と前記コンテンツの利用制限を解除するための認証情報 $AK$ （解除情報）とを含む情報を暗号化し、その暗号結果である暗号文 $C_{i,j}$ を、前記端末に送信する認証情報送信ステップと、を有し、

前記利用制限解除ステップは、

前記サーバから受信した暗号文 $C_{i,j}$ を前記記憶媒体から読み出した前記復号鍵 $K_i$ を用いて復号化し、その結果得られたユーザ情報 $ID$ を用いて、ユーザ認証を行う端末側ユーザ認証ステップと、

前記端末側ユーザ認証ステップでのユーザ認証が成立した場合に、前記暗号文 $C_{i,j}$ を復号化した結果得られた認証情報 $AK$ と、前記記憶媒体に記憶されている認証情報 $AK$ とを比較して、両者が一致する場合に、前記コンテンツの利用が制限されている部分へのアクセスを許可するアクセス許可ステップと、を有することを特徴とするコンテンツの利用制限解除方法。

【請求項14】請求項13記載のコンテンツの利用制限解除方法であって、

前記認証情報送信ステップは、

前記サーバ側ユーザ認証ステップでのユーザ認証が成立した場合に、乱数 $R$ を生成し、当該乱数 $R$ と前記認証情報 $AK$ と前記ユーザ情報 $ID$ とを、予め用意してある前記暗号鍵 $K_i$ を用いて暗号化し、その暗号結果である暗号文 $C_{i,j}$ を、前記端末に送信することを特徴とするコンテンツの利用制限解除方法。

【請求項15】請求項9記載のコンテンツの利用制限解除方法であって、

前記記憶媒体には、前記コンテンツと共に、非対称鍵暗号体系に従った当該コンテンツに固有の鍵であって、当該鍵からは、前記サーバが保持する当該鍵と対の暗号鍵

$K_{i,1}$ 、 $K_{i,2}$ を推測不可能な復号鍵 $K_{i,1}$ 、 $K_{i,2}$ と、当該コンテンツに固有の認証情報 $AK$ とが記憶されており、

前記解除情報送信ステップは、

前記端末より受信した解除依頼に含まれるユーザ情報 $ID$ を用いて、ユーザ認証を行うサーバ側ユーザ認証ステップと、

前記サーバ側ユーザ認証ステップでのユーザ認証が成立した場合に、予め用意してある前記暗号鍵 $K_{i,2}$ を用いて前記コンテンツの利用制限を解除するための認証情報 $AK$ （解除情報）を暗号化し、次いで、その暗号結果である

$C_{i,2}$ と前記端末より受信した解除依頼に含まれるユーザ情報 $ID$ とを、予め用意してある前記暗号鍵 $K_{i,1}$ を用いて暗号化し、その暗号結果である暗号文 $C_{i,j}$ を前記端末に送信する認証情報送信ステップと、を有し、

前記利用制限解除ステップは、

前記サーバから受信した暗号文 $C_{i,j}$ を前記記憶媒体から読み出した前記復号鍵 $K_{i,1}$ を用いて復号化し、その結果得られたユーザ情報 $ID$ を用いて、ユーザ認証を行う端末側ユーザ認証ステップと、

前記端末側ユーザ認証ステップでのユーザ認証が成立した場合に、前記暗号文 $C_{i,j}$ を復号化した結果得られた暗号文 $C_{i,2}$ を、前記記憶媒体から読み出した前記復号鍵 $K_{i,2}$ を用いて復号化して、認証情報 $AK$ を入手し、当該認証情報 $AK$ と、前記記憶媒体に記憶されている認証情報 $AK$ とを比較して、両者が一致する場合に、前記コンテンツの利用が制限されている部分へのアクセスを許可するアクセス許可ステップと、を有することを特徴とするコンテンツの利用制限解除方法。

【請求項16】記憶媒体が装着された端末にネットワークを介して接続されたサーバを用いて、当該記憶媒体に記憶されている、一部が利用可能であり、その他の部分の利用が制限されたコンテンツの利用制限を解除する、コンテンツの利用制限解除方法であって、

前記端末において、任意の情報を含む前記コンテンツの利用制限の解除依頼を生成し、前記サーバに送信する解除依頼ステップと、

前記サーバにおいて、前記端末から受信した解除依頼に含まれる情報に対するデジタル署名を生成し、これを解除情報として、前記端末に送信する解除情報送信ステップと、

前記端末において、前記サーバより解除情報として送られてきたデジタル署名を検証し、その正当性が確認できた場合に、前記コンテンツの利用が制限されている部分へのアクセスを許可するアクセス許可ステップと、を有することを特徴とするコンテンツの利用制限解除方法。

【請求項17】一部が利用可能であり、その他の部分の利用が制限されたコンテンツと、

ネットワークを介して接続されたサーバにアクセスし、当該サーバから前記コンテンツの利用制限を解除するための解除情報を入手して、当該コンテンツの利用制限を

解除するプログラムと、を格納したことを特徴とする記憶媒体。

【請求項 18】コンテンツが記憶された記憶媒体であって、  
前記コンテンツは、一部が利用可能であって、その他の部分の利用が制限されており、且つ、前記記憶媒体には、前記コンテンツの利用制限を解除する利用制限解除プログラムと、前記コンテンツに固有の鍵とが記憶されており、  
前記利用制限解除プログラムは、前記記憶媒体が装着された端末に読み取られて実行されることで、  
前記記憶媒体に記憶されている前記コンテンツに固有の鍵を用いた暗号通信により、当該端末にネットワークを介して接続されたサーバに、ユーザ情報ID<sub>i</sub>と鍵K<sub>i</sub>を含む解除依頼を送信する解除依頼手段と、  
前記コンテンツの利用制限を解除するための解除情報とユーザ情報ID<sub>i</sub>とを含む情報を前記鍵K<sub>i</sub>で暗号化することで得られる暗号文C<sub>i,j</sub>を、前記サーバから入手する解除情報入手手段と、  
前記解除情報入手手段で入手した暗号文C<sub>i,j</sub>を前記鍵K<sub>i</sub>で復号化し、その結果得られたユーザ情報ID<sub>i</sub>を用いてユーザ認証を行うユーザ認証手段と、  
前記ユーザ認証手段でのユーザ認証が成立した場合に、前記暗号文C<sub>i,j</sub>を復号化した結果得られた解除情報を用いて、前記コンテンツの利用制限を解除する利用制限解除手段とを、前記端末上に構築することを特徴とする記憶媒体。

【請求項 19】コンテンツが記憶された記憶媒体であって、  
前記コンテンツは、一部が利用可能であって、その他の部分の利用が制限されており、且つ、前記記憶媒体には、前記コンテンツの利用制限を解除する利用制限解除プログラムと、前記コンテンツに固有の鍵とあって当該鍵からは当該鍵と対の暗号鍵を推測不可能な鍵とが記憶されており、  
前記利用制限解除プログラムは、前記記憶媒体が装着された端末に読み取られて実行されることで、  
当該端末にネットワークを介して接続されたサーバに、ユーザ情報ID<sub>i</sub>を含む解除依頼を送信する解除依頼手段と、  
前記サーバから、前記コンテンツの利用制限を解除するための解除情報とユーザ情報ID<sub>i</sub>とを含む情報を前記暗号鍵で暗号化することで得られる暗号文C<sub>i,j</sub>を、入手する解除情報入手手段と、  
前記解除情報入手手段で入手した暗号文C<sub>i,j</sub>を、前記記憶媒体に記憶されている前記コンテンツに固有の鍵で復号化し、その結果得られたユーザ情報ID<sub>i</sub>を用いてユーザ認証を行うユーザ認証手段と、  
前記ユーザ認証手段でのユーザ認証が成立した場合に、前記暗号文C<sub>i,j</sub>を復号化した結果得られた解除情報を用

いて、前記コンテンツの利用制限を解除する利用制限解除手段とを、前記端末上に構築することを特徴とする記憶媒体。

【請求項 20】請求項 18 または 19 記載の記憶媒体であって、  
当該記憶媒体に記憶されるコンテンツに固有の鍵は、定期的に、もしくは、当該コンテンツが更新される都度、更新されることを特徴とする記憶媒体。  
【請求項 21】請求項 18、19 または 21 記載の記憶媒体であって、  
前記ユーザ認証手段は、前記端末が、前記記録媒体に記録されている前記コンテンツの利用が制限されている部分にアクセスする都度、実行され、  
前記利用制限解除手段は、前記ユーザ認証手段でのユーザ認証が成立する都度、前記端末がアクセスしようとしている部分についての利用制限を解除することを特徴とする記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、アプリケーションプログラムやマルチメディアデータ等のコンテンツの利用を制限する技術に関し、特に、ユーザに過度の負担をかけることなく、コンテンツの正規購入に先だってそのコンテンツを評価できるようにするのに好適な技術に関する。

【0002】

【従来の技術】近年、アプリケーションプログラムやマルチメディアデータ等のコンテンツが、CD-ROMやDVD-ROM等の記憶媒体に格納されて販売されている。この種のコンテンツは電子データであるため、ユーザは、コンテンツの評価などを行う雑誌で調べてみても、実際に使用してみないと、それが有益であるか否かを判断できないことが多い。このため、従来、この種の雑誌には、コンテンツの一部のみ利用可能にしたものが格納された記憶媒体、いわゆるお試し版が添付されたりしている。

【0003】

【発明が解決しようとする課題】しかしながら、上記の従来によれば、ユーザは、コンテンツの正規購入に先だってそのコンテンツを評価したい場合、本屋等でこの種の雑誌を購入し、それに添付されている前記コンテンツのお試し版を使用してみなければならない。そして、気に入った場合には、このお試し版とは別途に、ソフト販売店等で、前記コンテンツが格納された記憶媒体を購入しなければならない。つまり、上記の従来によれば、ユーザに、正規コンテンツの購入以外に、雑誌等購入の手間や金銭的な負担をかけている。

【0004】本発明は、上記事情に鑑みてなされたものであり、本発明の目的は、ユーザに過度の負担をかけることなく、コンテンツの正規購入に先だってそのコンテ



ンツを評価できるようにすることにある。

【0005】

【課題を解決するための手段】上記課題を解決するために、本発明では、アプリケーションプログラムやマルチメディアデータ等のコンテンツを、一部利用可能とし、その他の部分の利用を制限して、CD-ROMやDVD-ROM等の記憶媒体に格納し、ユーザに提供する。前記記憶媒体が装着されたネットワーク接続機能を有する端末は、ユーザの指示にしたがい、ネットワークを介してサーバにアクセスして、当該サーバから前記コンテンツの利用制限を解除するための解除情報を入手する。そして、当該解除情報を用いて前記コンテンツの利用制限を解除する。

【0006】本発明によれば、ユーザは、前記端末に前記記憶媒体を装着し、当該コンテンツの利用可能な部分を実際に使用してみて、当該コンテンツを評価することができる。ここで、CD-ROMやDVD-ROM等の記憶媒体自体の製造コストは、コンテンツ自体の対価に比べて安価である。したがって、そのままでは（解除情報を入手しなければ）一部しか利用できないコンテンツが格納された前記記憶媒体を、例えば、記録媒体自体の製造コストと流通コストを考慮した、比較的安価な値段でユーザに提供することができる。

【0007】また、ユーザは、前記コンテンツの利用可能な部分を実際に使用してみて、当該コンテンツを評価した結果、当該コンテンツを気に入った場合、当該コンテンツを格納した前記記憶媒体が装着された前記端末を用い、ネットワークを介してサーバにアクセスして、当該サーバから前記コンテンツの利用制限を解除するための解除情報を入手することにより、前記コンテンツの利用制限を解除することができる。つまり、ユーザは、全ての部分が利用可能に構成された正規のコンテンツが記憶された記憶媒体を別途購入しなくても済む。ここで、解除情報の対価は、例えば、前記コンテンツを格納する記憶媒体自体の製造コストと流通コストを除いた、当該コンテンツ自体に対する対価に設定することができる。

【0008】したがって、本発明によれば、ユーザに過度の負担をかけることなく、コンテンツの正規購入に先だってそのコンテンツを評価することが可能となる。つまり、上記の従来で説明したような、正規コンテンツの購入以外の雑誌等購入の手間や金銭的な負担を低減することができる。

【0009】なお、本発明において、前記記憶媒体が装着された前記端末が、ネットワークを介してサーバにアクセスして、当該サーバから前記コンテンツの利用制限を解除するための解除情報を入手し、当該コンテンツの利用制限を解除するためのプログラムは、前記コンテンツと共に前記記憶媒体に格納しておくようにするとよい。このようにすれば、前記端末自体に、前記サーバから解除情報を入手して前記コンテンツの利用制限を解除

するための専用のハードウェア構成を設ける必要がなくなる。つまり、ネットワーク接続機能を有するゲーム機やパーソナルコンピュータなどの汎用の電子計算機を前記端末に利用することが可能となる。

【0010】より具体的に説明すると、本発明の第1の態様では、記憶媒体が装着された端末にネットワークを介して接続されたサーバを用いて、当該記憶媒体に記憶されている、一部が利用可能であり、その他の部分の利用が制限されたコンテンツの利用制限を解除する、コンテンツの利用制限解除方法であって、前記端末において、前記コンテンツの利用制限の解除依頼を前記サーバに送信する解除依頼ステップと、前記サーバにおいて、前記端末より受信した解除依頼にしたがい、前記コンテンツの利用制限を解除するための解除情報を、当該コンテンツに固有の鍵を用いた暗号通信により前記端末と共有した鍵で暗号化し、前記端末に送信する解除情報送信ステップと、前記端末において、前記サーバより受信した暗号文を、前記記憶媒体に記憶されている前記コンテンツに固有の鍵を用いた暗号通信により、前記サーバと共有した鍵で復号化し、その結果得られた解除情報を用いて、前記コンテンツの利用制限を解除する利用制限解除ステップと、を有する。

【0011】本態様によれば、前記記憶媒体に前記コンテンツと共に記憶されている当該コンテンツに固有の鍵を用いて解除情報を、前記サーバから前記端末へ送信するようにしている。したがって、同じコンテンツであれば、当該コンテンツと共に前記記録媒体に記憶する鍵も同じものになる。つまり、記憶媒体毎に固有の情報を当該記憶媒体に記憶させる必要がないので、前記記憶媒体を例えばプレス等により大量生産するのに好適である。

【0012】また、本発明の第2の態様では、記憶媒体が装着された端末にネットワークを介して接続されたサーバを用いて、当該記憶媒体に記憶されている、一部が利用可能であり、その他の部分の利用が制限されたコンテンツの利用制限を解除する、コンテンツの利用制限解除方法であって、前記端末において、前記コンテンツの利用制限の解除依頼を前記サーバに送信する解除依頼ステップと、前記サーバにおいて、前記端末から受信した解除依頼にしたがい、前記コンテンツの利用制限を解除するための解除情報を、当該コンテンツに固有の暗号鍵で暗号化し、前記端末に送信する解除情報送信ステップと、前記端末において、前記サーバより受信した暗号文を、前記記憶媒体に記憶されている、前記コンテンツに固有の暗号鍵と対の復号鍵であって前記暗号鍵を推測不可能な復号鍵で、復号化し、その結果得られた解除情報を用いて、前記コンテンツの利用制限を解除する利用制限解除ステップと、を有する。

【0013】本態様においても、上記の第1の態様と同様、同じコンテンツであれば、当該コンテンツと共に前記記録媒体に記憶する鍵も同じものになるので、つま



り、記憶媒体毎に固有の情報を当該記憶媒体に記憶させる必要がないので、前記記憶媒体を例えばプレス等により大量生産するのに好適である。

【0014】加えて、本態様によれば、前記記憶媒体に記憶される鍵を、当該鍵からは前記サーバが保持する対の暗号鍵を推測不可能な復号鍵としている。したがって、例えば不正な第3者が前記記憶媒体の内容を解析して前記復号鍵を入手したとしても、当該復号鍵からこれと対の暗号鍵を求めることができない以上、当該第3者が、前記復号鍵で復号可能な解除情報を含む暗号文を生成することはできない。つまり、当該第3者が前記サーバの運営者になりすますのを防ぐことができる。

【0015】

【発明の実施の形態】まず、以下に説明する本発明の各実施形態が適用されるコンテンツ利用制限解除システムの概略について、図1を用いて説明する。

【0016】図1は、本発明の各実施形態が適用されるコンテンツ利用制限解除システムの概略構成図である。

【0017】図示するように、このコンテンツ利用制限解除システムは、ユーザ端末1と、ソフトメカ5もしくはソフトメカ5からの依頼を受けた者が運営する解除情報配信センタ2とが、ネットワーク3を介して、互いに接続されて構成されている。なお、ここでは、ユーザ端末1および解除情報配信センタ2をそれぞれ1つ示しているが、当然のことながら、複数であっても構わない。

【0018】ソフトメカ5は、一部を利用可能とし、その他の部分の利用を何らかの方法により制限した、アプリケーションプログラム（例えばゲーム）やマルチメディアデータ（例えばビデオ）等のコンテンツを、その利用制限を解除するための利用制限解除プログラムと共に、CD-ROMやDVD-ROM等の記憶媒体4に格納して、例えばソフト販売店6等経由でユーザ7に提供する。また、コンテンツの利用制限を解除するための解除情報とそのコンテンツのタイトル名とを、暗号通信や郵送等のセキュリティが確保される方法により、解除情報配信センタ2に知らせる。解除情報配信センタ2は、ソフトメカ5から通知されたコンテンツのタイトル名とその解除情報とを対応付けて記憶装置等に記憶し管理する。

【0019】なお、CD-ROMやDVD-ROM等の記憶媒体4自体の製造コストは、コンテンツの対価に比べて安価であり、また、記憶媒体4に格納されているコンテンツは、そのままでは（解除情報を入手しなければ）一部しか利用できないものであるため、記録媒体4の値段を、例えば、記録媒体4自体の製造コストと当該記録媒体4の流通コストとを考慮した、比較的安価な値段に設定し、ユーザ7に提供することができる。

【0020】ユーザ7は、ソフト販売店6等で購入した記憶媒体4を、ユーザ端末1に装着し、当該記憶媒体4

に格納されているコンテンツの利用可能な部分を実際に試してみても、当該コンテンツを評価することができる。気に入った場合には、ユーザ端末1に、当該記録媒体4中に格納されている利用制限解除プログラムを起動させることにより、ネットワーク3を介して解除情報配信センタ2に前記コンテンツのタイトル名を含む解除依頼を送信し、解除情報配信センタ2から当該コンテンツの解除情報を購入することができる。そして、この利用制限解除プログラムにより、購入した解除情報を使って対応するコンテンツの利用制限を解除することで、コンテンツの全ての部分が利用可能になる。

【0021】なお、解除情報の値段は、例えば記憶媒体4自体の製造コストと記録媒体4の流通コストを除いたコンテンツ自体の値段に設定することができる。したがって、従来の技術で説明したような、正規コンテンツの購入以外の雑誌等購入の手間や金銭的な負担をユーザにかけなくて済む。

【0022】また、解除情報配信センタ2に解除依頼を送信して解除情報を購入し、コンテンツの利用制限を解除するための利用制限解除プログラムは、当該コンテンツと共に記録媒体4に格納されているので、ユーザ端末1にそのための専用ハードウェア構成を設ける必要がなくなる。つまり、ネットワーク接続機能を有するテレビゲーム機やパーソナルコンピュータなどの汎用の電子計算機をユーザ端末1として利用することが可能となる。

【0023】以下に、上述したコンテンツ利用制限解除システムの、より具体的な実施形態について説明する。

【0024】まず、本発明の第1実施形態について説明する。

【0025】本実施形態では、記憶媒体4に格納するコンテンツの利用制限を暗号化により実現している。そして、当該コンテンツの暗号化部分を復号するための復号鍵（解除情報）を、共通鍵暗号体系に従った当該コンテンツに固有の鍵情報を用いた、暗号通信により、解除情報配信センタ2からユーザ端末1へ送信するようにしている。

【0026】まず、記憶媒体4のデータ構成について説明する。

【0027】図2は、本実施形態で用いられる記憶媒体4のデータ構成図である。

【0028】図示するように、記憶媒体4には、コンテンツ41と利用制限解除プログラム42が格納される。コンテンツ41は、ゲーム等のアプリケーションプログラム411と、そのアプリケーションプログラム411が使用するアプリケーションデータ412とを有する。アプリケーションデータ412は、一部を残してその他の部分が暗号化されている。また、利用制限解除プログラム42は、鍵生成プログラム421と、鍵情報入手プログラム422と、コンテンツ復号化プログラム423と、共通鍵暗号体系に従った、コンテンツ41に固有の

鍵情報GK424と、を有する。なお、ここでは、いわゆるバージョンの相違も異なるコンテンツとみなしている。

【0029】次に、ユーザ端末1について説明する。

【0030】図3に、ユーザ端末1のハードウェア構成の一例を示す。

【0031】なお、上述したように、ユーザ端末1には、ネットワーク接続機能を有するテレビゲーム機やパーソナルコンピュータなどの汎用の電子計算機を利用することができる。ここでは、ユーザ端末1がテレビゲーム機である場合の一例を示している。

【0032】図3において、CPU11は、本ユーザ端末1の各部を統括的に制御する。メモリ12は、CPU11のワークエリアとして機能する。フラッシュメモリ13には、オペレーティングシステム(OS)プログラムと、本ユーザ端末1の識別情報ID<sub>u</sub>とが格納されている。また、本ユーザ端末1のユーザより受け付けたユーザの個人情報ID<sub>u</sub>が格納される。

【0033】通信装置14は、ネットワーク3を介して、解除情報配信センタ2にアクセスし、解除情報配信センタ2から解除情報(コンテンツ41を復号するための鍵)入手するのに用いられる。

【0034】入力装置16は、各種操作ボタンを備えたコントローラで構成され、ユーザからのコンテンツ41の利用指示や解除情報の入手指示等を受け付ける。

【0035】読取装置19には、記憶媒体4が装着され、当該記憶媒体4から利用制限解除プログラム42やコンテンツ41を読み出す。

【0036】オーディオ再生装置16は、読取装置19より読み出されたコンテンツ41を再生してオーディオ信号を生成する。また、CPU12からの指示にしたがい、図示していないサウンドバッファに格納されている波形データ等を利用してオーディオ信号を生成する。

【0037】ビデオ再生装置17は、読取装置19より読み出されたコンテンツ41を再生してビデオ信号を生成する。また、CPU12からの描画指示にしたがい、図示していないテクスチャバッファに格納されているテクスチャデータ等を利用して描画を行い、そのビデオ信号を生成する。

【0038】カード接続装置18は、メモリカード20を接続し、当該メモリカード20に解除情報を格納したり、当該メモリカード30に格納された解除情報を読み出ししたりする。

【0039】インターフェース21は、CPU11やメモリ12やフラッシュメモリ13と本ユーザ端末1を構成する他装置との間のデータ送受を司る。

【0040】図4に、ユーザ端末1上に構築されるソフトウェア構成を示す。

【0041】この図に示す各構成要素は、フラッシュメモリ13に格納されているOSプログラムが稼動してい

る状態で、読取装置19により記憶媒体4から読み出され、メモリ12上にロードされた、利用制限解除プログラム42およびアプリケーションプログラム411を、CPU11が実行することにより、プロセスとして具現化される。

【0042】鍵生成部111は、鍵生成プログラム421により実現される。乱数を生成して鍵K<sub>i</sub>を生成する。

【0043】解除情報入手部112は、解除情報入手プログラム421により実現される。記憶媒体4に格納されている鍵情報GKを用いた共通鍵暗号による暗号通信により、解除情報配信センタ2よりコンテンツ41復号化のための鍵K(解除情報)を入手する。

【0044】コンテンツ復号化部113は、コンテンツ復号化プログラム423により実現される。解除情報入手部112で入手した鍵Kを用いて、記憶媒体4に格納されているアプリケーションデータ412の暗号化部分を復号する。

【0045】アプリ処理部115は、アプリケーションプログラム411により実現され、アプリケーションプログラム411の内容に応じた処理(たとえば、アプリケーションプログラム411がゲームプログラムならばゲームの実行)を行う。

【0046】主制御部114は、OSにより実現され、図3に示す本ユーザ端末1の各ハードウェア構成要素を統括的に制御する。また、鍵生成部111や解除情報入手部112やコンテンツ復号化部113やアプリ処理部115に指示を出す。

【0047】次に、解除情報配信センタ2について説明する。

【0048】解除情報配信センタ2のハードウェア構成は、例えば、図3において、オーディオ再生装置16やビデオ再生装置17やカード接続装置18やフラッシュメモリ19が省略され、その代わりにハードディスク等の記憶装置が設けられた、一般的な構成を有する電子計算機を利用することができる。

【0049】図5に、解除情報配信センタ2上に構築されるソフトウェア構成を示す。

【0050】解除情報送信部211は、後述する管理テーブル212に格納されている鍵情報GKを用いた共通鍵暗号による暗号通信により、コンテンツ復号化のための鍵K(解除情報)を送信する。

【0051】管理テーブル212には、ソフトメカ5より通知されたコンテンツ41のタイトル名212aと、そのバージョン名212bと、タイトル名212aおよびバージョン名212bにより特定されるコンテンツ41にユニークに割り当てられた、共通鍵暗号体系に従った鍵情報GK212cと、当該コンテンツ41の暗号化部分を復号するための鍵K212dが、互いに対応付けられて、リスト形式で登録・管理されている。

【0052】課金処理部213は、解除情報送信部21

1にてコンテンツ41復号化のための鍵K212dを送信したユーザ端末1のユーザに対する課金処理を行う。

【0053】なお、上記の解除情報送信部211や課金処理部213は、予めハードディスク等の記憶装置に格納されているOSが稼動している状態で、所定のプログラムが前記記憶装置あるいは読取装置を介して記憶媒体から読み出されてメモリ上にロードされ、それをCPUが実行することにより、プロセスとして具現化される。また、管理テーブル212には、前記記憶装置等が利用される。

【0054】次に、本実施形態の動作について説明する。

【0055】本実施形態の動作は、ユーザ端末1において、鍵情報配信センタ2に送信する解除依頼中に含める情報を生成する解除依頼生成処理、ユーザ端末1が、前記解除依頼生成処理で生成した情報を含んだ解除依頼を鍵情報配信センタ2に送信して、鍵情報配信センタ2から鍵K(解除情報)を入手する解除情報入手処理、および、入手した鍵Kを用いてコンテンツ41の暗号化部分を復号化するコンテンツ復号化処理の3つに分けられる。

【0056】まず、解除依頼生成処理について説明する。

【0057】図6は、本実施形態の解除依頼生成処理を説明するための図である。

【0058】ユーザ端末1において、主制御部114は、入力装置15を介してユーザより解除依頼生成の指示を受け付けると、鍵生成部111に指示を出す。これを受けて、鍵生成部111は、乱数により鍵K<sub>i</sub>を生成し、これを解除情報入手部112に渡す(ステップS1001)。

【0059】次に、解除情報入手部112は、主制御部114を介して、フラッシュメモリ13からユーザの個人情報ID<sub>i</sub>を読み出すと共に、記憶媒体4から鍵情報CK424を読み出す。そして、共通鍵暗号体系にしたがい、鍵生成部111から受け取った鍵K<sub>i</sub>とユーザの個人情報ID<sub>i</sub>とを繋げたデータ(K<sub>i</sub> || ID<sub>i</sub>)を、鍵情報CK424を用いて暗号化し、暗号文C<sub>i,j</sub>(=E<sub>K<sub>i</sub></sub>(K<sub>i</sub> || ID<sub>i</sub>))を生成する(ステップS1002)。

【0060】次いで、解除情報入手部112は、生成した暗号文C<sub>i,j</sub>を、主制御部114を介してメモリカード20に格納し(ステップS1003)、その後、メモリ12上のワークエリアから鍵K<sub>i</sub>を除去して処理を終了する(ステップS1004)。

【0061】次に、解除情報入手処理について説明する。

【0062】図7および図8は、本実施形態の解除情報入手処理を説明するための図であり、図7はユーザ端末1側での処理を、そして、図8は鍵情報配信センタ2側での処理を示している。

【0063】まず、ユーザ端末1において(図7参照)、主制御部114は、入力装置15を介してユーザより解除情報入手の指示を受け付けると、解除情報入手部112に指示を出す。これを受けて、解除情報入手部112は、主制御部114を介して、フラッシュメモリ13からユーザの個人情報ID<sub>i</sub>を読み出すと共に、記憶媒体4からコンテンツ41のタイトルおよびバージョン名を読み出す。また、メモリカード20から、解除依頼生成処理で作成した暗号文C<sub>i,j</sub>(=E<sub>K<sub>i</sub></sub>(K<sub>i</sub> || ID<sub>i</sub>))を読み出す。そして、ユーザの個人情報ID<sub>i</sub>、コンテンツのタイトルおよびバージョン名、および、暗号文C<sub>i,j</sub>を含んだ解除依頼を作成し(ステップS1101)、解除情報配信センタ2に送信する(ステップS1102)。

【0064】解除情報配信センタ2において(図8参照)、解除情報送信部211は、ユーザ端末1より解除依頼を受信すると(ステップS1201)、当該解除依頼に含まれているコンテンツのタイトルおよびバージョン名に対応する鍵情報CK212c(これは当該コンテンツを格納する記憶媒体4の利用制限解除プログラム42に格納されている鍵情報CK424と一致する)を読み出し、この鍵情報CKを用いて、前記解除依頼に含まれている暗号文C<sub>i,j</sub>を復号化する。これにより、鍵K<sub>i</sub>とユーザの個人情報ID<sub>i</sub>を得る(ステップS1202)。

【0065】それから、課金処理部213は、解除依頼を送信したユーザ端末1のユーザの認証を行う(ステップS1203)。例えば、受信した解除依頼に含まれているユーザの個人情報ID<sub>i</sub>が正規のユーザとして記憶装置等に登録されているか否かを調べ、登録されているならば、当該個人情報ID<sub>i</sub>とステップS1202で暗号文C<sub>i,j</sub>を復号化した結果得られたユーザの個人情報ID<sub>i</sub>とを比較する。そして、両者が一致する場合は、ユーザ認証が成立したものとする。

【0066】ユーザ認証が成立しなかった場合(ステップS1204でNo)は、その旨を解除情報送信部211に知らせて、前記解除依頼を送信したユーザ端末1にエラー通知を送信する(ステップS1205)。

【0067】一方、ユーザ認証が成立した場合(ステップS1204でYes)は、そのユーザの個人情報ID<sub>i</sub>により特定されるユーザに対して課金処理を行い(ステップS1206)、その旨を解除情報送信部211に知らせる。解除情報送信部211は、受信した解除依頼に含まれているコンテンツのタイトルおよびバージョン名に対応する鍵K212d(これが当該タイトルおよびバージョン名により特定されるコンテンツ41のアプリケーションデータ412の暗号化部分を復号化するための鍵(解除情報)である)を読み出し、この鍵Kと前記ユーザの個人情報ID<sub>i</sub>とを繋げたデータ(K || ID<sub>i</sub>)を、ステップS1202で暗号文C<sub>i,j</sub>を復号化した結果得られた鍵K<sub>i</sub>を用いて暗号化し、暗号文C<sub>i,j</sub>(=E<sub>K<sub>i</sub></sub>(K || ID<sub>i</sub>))を生成して(ステップS1207)、前記解除依頼を送信

したユーザ端末1に送信する(ステップS1208)。  
 【0068】ユーザ端末1において(図7参照)、解除情報入手部112は、解除情報配信センタ2より情報を受信すると(ステップS1103)、それがエラー通知ならば(ステップS1104でNo)、その旨を本ユーザ端末1に接続されているテレビ等に出力するなど所定のエラー処理を行う(ステップS1105)。一方、暗号文C<sub>1,1</sub>ならば(ステップS1104でYes)、記憶媒体4から鍵情報CK424を読み出すと共に、メモリカード20から、解除依頼生成処理で作成した暗号文C<sub>1,1</sub> (=E<sub>k</sub>(K<sub>1</sub>||ID<sub>1</sub>))を読み出す。そして、この鍵情報CKを用いて暗号文C<sub>1,1</sub>を復号化し、鍵K<sub>1</sub>とユーザの個人情報ID<sub>1</sub>を得る(ステップS1106)。次に、この鍵K<sub>1</sub>を用いて、鍵情報配信センタ2より受信した暗号文C<sub>1,1</sub> (=E<sub>k</sub>(K<sub>1</sub>||ID<sub>1</sub>))を復号化し、コンテンツ41復号化のための鍵Kとユーザの個人情報ID<sub>1</sub>を得る(ステップS1107)。  
 【0069】それから、解除情報入手部112は、ステップS1106で暗号文C<sub>1,1</sub>を復号化することで得たユーザの個人情報ID<sub>1</sub>と、ステップS1107で暗号文C<sub>1,1</sub>を復号化することで得たユーザの個人情報ID<sub>1</sub>とを比較し、両者の一致を調べることで、ユーザ認証を行う(ステップS1108)。  
 【0070】ユーザ認証が成立しなかった場合(ステップS1109でNo)は、その旨を本ユーザ端末1に接続されているテレビ等に出力するなど所定のエラー処理を行い、それから、メモリ12上のワークエリアから鍵K<sub>1</sub>を除去して処理を終了する(ステップS1105)。  
 【0071】一方、ユーザ認証が成立した場合(ステップS1109でYes)は、鍵情報配信センタ2より受信した暗号文C<sub>1,1</sub>を、主制御部114を介してメモリカード20に、当該メモリカード20に既に格納されている暗号文C<sub>1,1</sub>と共に格納し(ステップS1110)、それから、メモリ12上のワークエリアから鍵K<sub>1</sub>を除去して処理を終了する(ステップS1111)。  
 【0072】次に、コンテンツ復号化処理について説明する。  
 【0073】図9は、本実施形態のコンテンツ復号化処理を説明するための図である。  
 【0074】ユーザ端末1において、コンテンツ復号化部113は、アプリ処理部115によるアプリケーションデータ412の暗号化部分へのアクセスを監視する(ステップS1301)。そして、アプリ処理部115がアプリケーションデータ412の暗号化部分へアクセスし、主制御部114が暗号化データを読み出した場合には、これをフェッチする。  
 【0075】次に、コンテンツ復号化部113は、主制御部114を介して、メモリカード20から暗号文C<sub>1,1</sub>を読み出すと共に、記憶媒体4から鍵情報CK424を説出。そして、この鍵情報CKを用いて暗号文C<sub>1,1</sub>を復号

化することにより、鍵K<sub>1</sub>とユーザの個人情報ID<sub>1</sub>を得る(ステップS1302)。  
 【0076】それから、コンテンツ復号化部113は、主制御部114を介してフラッシュメモリ13からユーザの個人情報ID<sub>1</sub>を読み出して、これとステップS1302で暗号文C<sub>1,1</sub>を復号化することで得たユーザの個人情報ID<sub>1</sub>とを比較し、両者の一致を調べることで、ユーザ認証を行う(ステップS1303)。  
 【0077】ユーザ認証が成立しなかった場合(ステップS1304でNo)は、ステップS1301でフェッチした暗号化データをアプリ処理部115に渡し、その後、メモリ12上のワークエリアから鍵K<sub>1</sub>を除去して、ステップS1301に戻る。  
 【0078】一方、ユーザ認証が成立した場合(ステップS1304でYes)は、主制御部114を介してメモリカード20から暗号文C<sub>1,1</sub>を読み出し、これをステップS1302で得た鍵K<sub>1</sub>を用いて復号化し、コンテンツ復号化のための鍵Kとユーザの個人情報ID<sub>1</sub>を得る(ステップS1305)。  
 【0079】それから、コンテンツ復号化部113は、ステップS1302で暗号文C<sub>1,1</sub>を復号化することで得たユーザの個人情報ID<sub>1</sub>と、ステップS1305で暗号文C<sub>1,1</sub>を復号化することで得たユーザの個人情報ID<sub>1</sub>とを比較し、両者の一致を調べることで、ユーザ認証を行う(ステップS1306)。  
 【0080】ユーザ認証が成立しなかった場合(ステップS1307でNo)は、ステップS1301でフェッチした暗号化データをアプリ処理部115に渡し、その後、メモリ12上のワークエリアから鍵K<sub>1</sub>を除去して、ステップS1301に戻る。  
 【0081】一方、ユーザ認証が成立した場合(ステップS1307でYes)は、ステップS1301でフェッチした暗号化データを、ステップS1305で得た鍵K<sub>1</sub>を用いて復号化する(ステップS1308)。そして、復号化したデータをアプリ処理部115に渡した後、メモリ12上のワークエリアから鍵K<sub>1</sub>を除去して、ステップS1301に戻る。  
 【0082】以上、本発明の第1実施形態について説明した。  
 【0083】本実施形態によれば、記憶媒体4にコンテンツ41と共に記憶されている当該コンテンツ41に固有の鍵情報CKと、ユーザ端末1のユーザの個人情報ID<sub>1</sub>とを用いて、当該ユーザ端末1のユーザのみが利用できる(ユーザ認証をパスできる)解除情報(鍵K)を、解除情報配信センタ2からユーザ端末1へ送信するようにしている。したがって、タイトル名およびバージョンが同じコンテンツ41であれば、当該コンテンツ41と共に記録媒体4に記憶する鍵情報CKも同じものになる。つまり、記憶媒体4毎に固有の情報を当該記憶媒体4に記憶させる必要がないので、CD-ROMやDVD-ROM等

の記憶媒体4を、例えばプレス等により大量生産するのに好適である。

【0084】また、ユーザ端末1において、コンテンツ復号化部113は、アプリ処理部115によるアプリケーションデータ412の暗号化部分へのアクセスを監視し、前記アクセスがあった場合に、主制御部114を介して記憶媒体4から読み出された暗号化データを復号化するようにしている。つまり、アプリケーションデータ412の暗号化部分の復号を、アプリ処理部115での処理中に、アプリ処理部115が要求するアプリケーションデータ412が暗号化されているか否かに応じてダイナミックに行うことができる。

【0085】なお、上記の第1実施形態では、ユーザ端末1が解除情報配信センタ2に送信する解除情報に含まれる暗号文 $C_{i,j}$ を、鍵生成部111から受け取った鍵 $K_i$ とユーザの個人情報 $ID_i$ とを繋げたデータ( $K_i \parallel ID_i$ )を鍵情報 $GK_{424}$ で暗号化することで作成している。しかしながら、鍵 $K_i$ とユーザの個人情報 $ID_i$ にその他のデータを繋げたデータを鍵情報 $GK_{424}$ で暗号化することで、暗号文 $C_{i,j}$ を作成するようにしてもよい。

【0086】例えば、ユーザ端末1のフラッシュメモリ13等にユーザ端末1の識別情報 $ID_i$ が格納されている場合は、鍵 $K_i$ とユーザの個人情報 $ID_i$ とユーザ端末1の識別情報 $ID_i$ とを繋げたデータ( $K_i \parallel ID_i \parallel ID_i$ )を、鍵情報 $GK_{424}$ を用いて暗号化して、暗号文 $C_{i,j}$ を作成するようにしてもよい。そして、この識別情報 $ID_i$ を解除依頼に加えて解除情報配信センタ2に送信し、当該解除情報配信センタ2において、ユーザの個人情報 $ID_i$ に加えてユーザ端末1の識別情報 $ID_i$ をも利用して、ユーザ認証を行うようにしてもよい。

【0087】あるいは、鍵生成部111に鍵 $K_i$ と共に乱数 $R$ を生成させ、鍵 $K_i$ とユーザの個人情報 $ID_i$ と乱数 $R$ を繋げたデータ( $K_i \parallel ID_i \parallel R$ )を、鍵情報 $GK_{424}$ を用いて暗号化して、暗号文 $C_{i,j}$ を作成するようにしてもよい。このようにすれば、暗号文 $C_{i,j}$ から鍵 $K_i$ が不正に解読される可能性をより低くできる。

【0088】また、解除情報配信センタ2からユーザ端末1へ送信される暗号文 $C_{i,j}$ についても同様に、例えば解除情報送信部211に乱数 $R$ を生成させ、鍵 $K_i$ とユーザの個人情報 $ID_i$ と乱数 $R$ を繋げたデータ( $K_i \parallel ID_i \parallel R$ )を、鍵 $K_i$ を用いて暗号化することで、作成するようにしてもよい。このようにすれば、暗号文 $C_{i,j}$ から鍵 $K_i$ が不正に解読される可能性をより低くできる。

【0089】また、上記の第1実施形態では、コンテンツのタイトルのみならずバージョンが異なる場合でも、鍵情報 $GK$ が異なるようにしているが、これに限定されない。例えば、コンテンツのタイトルが同じであれば、バージョンにかかわらず同じ鍵情報 $GK$ を用いるようにしてもかまわない。あるいは、同じコンテンツのタイトルに対して、出荷時期等を考慮して、定期的に鍵情報 $GK$ を変

えるようにしてもよい。この場合、コンテンツ41に当該コンテンツ41の出荷時期がわかるような時期情報を入れておき、解除依頼にこの時期情報を含めて、ユーザ端末1から解除情報配信センタ2に送信する。そして、解除情報配信センタ2は、管理テーブル212において、鍵情報 $GK$ をコンテンツのタイトル名と時期情報とで管理することで、解除情報に含まれるコンテンツのタイトル名および時期情報から、当該解除情報に含まれる暗号文 $C_{i,j}$ を復号化するのに用いる鍵情報 $GK$ を、特定することができる。

【0090】次に、本発明の第2実施形態について説明する。

【0091】上記の第1実施形態では、ユーザ端末1は、解除情報配信センタ2に送信する解除情報に含まれる暗号文 $C_{i,j}$ を、鍵生成部111から受け取った鍵 $K_i$ とユーザの個人情報 $ID_i$ とを繋げたデータ( $K_i \parallel ID_i$ )を鍵情報 $GK_{424}$ を用いて暗号化することで作成している。このため、解除情報配信センタ2において、ユーザ認証を行う前の時点で、鍵 $K_i$ の内容が明らかになってしまう(図8のステップS1202、ステップS1203参照)。一方、解除情報配信センタ2は、ユーザ端末1に送信する暗号文 $C_{i,j}$ を、コンテンツ復号化のための鍵 $K_i$ とユーザの個人情報 $ID_i$ とを繋げたデータ( $K_i \parallel ID_i$ )を鍵 $K_i$ を用いて暗号化することで作成している。このため、ユーザ端末1において、ユーザ認証を行う前の時点で、鍵 $K_i$ が取得されてしまう(図7のステップS1107、ステップS1108参照)。

【0092】そこで、本実施形態では、解除情報配信センタ2において、ユーザ認証を行う前の時点で、鍵 $K_i$ の内容が明らかにならないように、多重に暗号化を施して暗号文 $C_{i,j}$ を作成すると共に、ユーザ端末1において、ユーザ認証を行う前の時点で、鍵 $K_i$ の内容が明らかにならないように、多重に暗号化を施して暗号文 $C_{i,j}$ を作成するようにして、セキュリティを強化している。

【0093】図10は、本実施形態で用いられる記憶媒体4のデータ構成図である。

【0094】ここで、図2に示す第1実施形態と同じ機能を有するものには、同じ符号を付している。図示するように、本実施形態では、利用制限解除プログラム42に、共通鍵暗号体系に従った、コンテンツ41に固有の3つの鍵情報 $GK_{424a}$ 、 $GK_{424b}$ 、 $GK_{424c}$ を格納している。

【0095】なお、ユーザ端末1のハードウェア構成やソフトウェア構成は、図3および図4に示す第1実施形態とものと同様である。また、解除情報配信センタ2のハードウェア構成やソフトウェア構成も、基本的に第1実施形態のものと同様であるが、図11に示すように、管理テーブル212に、タイトル名212aおよびバージョン名212bにより特定されるコンテンツ41に固有の3つの鍵情報 $GK_{212e}$ 、 $GK_{212f}$ 、 $GK_{212g}$

10

20

30

40

50

2gを格納している点が異なる。

【0096】次に、本実施形態の動作について説明する。

【0097】本実施形態の動作も、上記の第1実施形態と同様に、解除依頼生成処理、解除情報入手処理およびコンテンツ復号化処理の3つに分けられる。

【0098】まず、解除依頼生成処理について説明する。

【0099】図12は、本実施形態の解除依頼生成処理を説明するための図である。

【0100】ユーザ端末1において、主制御部114は、入力装置15を介してユーザより解除依頼生成の指示を受け付けると、鍵生成部111に指示を出す。これを受けて、鍵生成部111は、乱数により鍵 $K_1$ 、 $K_2$ を生成し、これを解除情報入手部112に渡す(ステップS2001)。

【0101】次に、解除情報入手部112は、主制御部114を介して、フラッシュメモリ13からユーザの個人情報ID<sub>i</sub>を読み出すと共に、記憶媒体4から3つの鍵情報GK<sub>212e</sub>、GK<sub>212f</sub>、GK<sub>212g</sub>を読み出す。そして、共通鍵暗号体系にしたがい、鍵生成部111から受け取った鍵 $K_1$ を鍵情報GK<sub>212g</sub>で暗号化し、その結果( $E_{K_1}(K_2)$ )に鍵生成部111から受け取った鍵 $K_2$ を繋げたデータ( $E_{K_1}(K_2) \| K_1$ )を、鍵情報GK<sub>212f</sub>でさらに暗号化する。そして、さらにその結果( $E_{K_1}(E_{K_2}(K_2) \| K_1)$ )に、ユーザの個人情報ID<sub>i</sub>を繋げたデータ( $E_{K_1}(E_{K_2}(K_2) \| K_1) \| ID_i$ )を、GK<sub>212e</sub>で暗号化する。これにより、暗号文C<sub>11</sub>(= $E_{K_1}(E_{K_2}(E_{K_3}(K_2) \| K_1) \| ID_i)$ )を生成する(ステップS2002)。

【0102】次いで、解除情報入手部112は、生成した暗号文C<sub>11</sub>を、主制御部114を介してメモリカード20に格納し(ステップS2003)、その後、メモリ12上のワークエリアから鍵 $K_1$ 、 $K_2$ を除去して処理を終了する(ステップS2004)。

【0103】次に、解除情報入手処理について説明する。

【0104】図13および図14は、本実施形態の解除情報入手処理を説明するための図であり、図13はユーザ端末1側での処理を、そして、図14は鍵情報配信センタ2側での処理を示している。

【0105】まず、ユーザ端末1において(図13参照)、主制御部114は、入力装置15を介してユーザより解除情報入手の指示を受け付けると、解除情報入手部112に指示を出す。これを受けて、解除情報入手部112は、主制御部114を介して、フラッシュメモリ13からユーザの個人情報ID<sub>i</sub>を読み出すと共に、記憶媒体4からコンテンツ41のタイトルおよびバージョン名を読み出す。また、メモリカード20から、解除依頼生成処理で作成した暗号文C<sub>11</sub>(= $E_{K_1}(E_{K_2}(E_{K_3}(K$

$K_1) \| K_1) \| ID_i$ )を読み出す。そして、ユーザの個人情報ID<sub>i</sub>とコンテンツのタイトルおよびバージョン名と暗号文C<sub>11</sub>を含んだ解除依頼を作成し(ステップS2101)、解除情報配信センタ2に送信する(ステップS2102)。

【0106】解除情報配信センタ2において(図14参照)、解除情報送信部211は、ユーザ端末1より解除依頼を受信すると(ステップS2201)、管理テーブル212から、当該解除依頼に含まれているコンテンツのタイトルおよびバージョン名に対応する鍵情報GK<sub>212e</sub>(これは当該コンテンツを格納する記憶媒体4の利用制限解除プログラム42に格納されている鍵情報GK<sub>424a</sub>と一致する)を読み出し、この鍵情報GK<sub>212e</sub>を用いて、前記解除依頼に含まれている暗号文C<sub>11</sub>を復号化する。これにより、ユーザの個人情報ID<sub>i</sub>を得る(ステップS2202)。

【0107】それから、課金処理部213は、解除依頼を送信したユーザ端末1のユーザの認証を行う(ステップS2203)。例えば、受信した解除依頼に含まれているユーザの個人情報ID<sub>i</sub>が正規のユーザとして記憶装置等に登録されているか否かを調べ、登録されているならば、当該個人情報ID<sub>i</sub>とステップS1202で得たユーザの個人情報ID<sub>i</sub>とを比較する。そして、両者が一致する場合は、ユーザ認証が成立したものとする。

【0108】ユーザ認証が成立しなかった場合(ステップS2204でNo)は、その旨を解除情報送信部211に知らせ、前記解除依頼を送信したユーザ端末1にエラー通知を送信する(ステップS2205)。

【0109】一方、ユーザ認証が成立した場合(ステップS2204でYes)は、そのユーザの個人情報ID<sub>i</sub>により特定されるユーザに対して課金処理を行い(ステップS2206)、その旨を解除情報送信部211に知らせる。解除情報送信部211は、管理テーブル212から、前記解除依頼に含まれているコンテンツのタイトルおよびバージョン名に対応する鍵情報GK<sub>212f</sub>、GK<sub>212g</sub>(これは当該コンテンツを格納する記憶媒体4の利用制限解除プログラム42に格納されている鍵情報GK<sub>424b</sub>、GK<sub>424c</sub>と一致する)を読み出し、この鍵情報GK<sub>212f</sub>、GK<sub>212g</sub>を用いて、ステップS2202で暗号文C<sub>11</sub>を復号化した結果得られたデータ( $E_{K_1}(E_{K_2}(K_2) \| K_1)$ )を復号化する。これにより、鍵 $K_1$ 、 $K_2$ を得る(ステップS2207)。

【0110】それから、解除情報送信部211は、管理テーブル212から、受信した解除依頼に含まれているコンテンツのタイトルおよびバージョン名に対応する鍵K<sub>212d</sub>(これが当該タイトルおよびバージョン名により特定されるコンテンツ41のアプリケーションデータ412の暗号化部分を復号化するための鍵(解除情報)である)を読み出し、この鍵K<sub>212d</sub>を前記鍵 $K_1$ で暗号化し、さらにその結果と前記ユーザの個人情報ID<sub>i</sub>とを繋



げたデータ( $E_{k_1}(K) \parallel ID_k$ )を、前記鍵 $K_{k_1}$ で暗号化して、暗号文 $C_{k_1}$ ( $=E_{k_1}(E_{k_1}(K) \parallel ID_k)$ )を生成し(ステップS2208)、前記解除依頼を送信したユーザ端末1に送信する(ステップS2209)。

【0111】ユーザ端末1において(図13参照)、解除情報入手部112は、解除情報配信センタ2より情報を受信すると(ステップS2103)、それがエラー通知ならば(ステップS2104でNo)、その旨を本ユーザ端末1に接続されているテレビ等に出力するなど所定のエラー処理を行う(ステップS2105)。一方、暗号文 $C_{k_1}$ ならば(ステップS2104でYes)、記憶媒体4から鍵情報 $CK_{k_1}$ 424a、 $CK_{k_1}$ 424bを読み出すと共に、メモリカード20から、解除依頼生成処理で作成した暗号文 $C_{k_1}$ ( $=E_{k_1}(E_{k_1}(K_{k_1}) \parallel ID_k)$ )を読み出す。そして、この鍵情報 $CK_{k_1}$ を用いて暗号文 $C_{k_1}$ を復号化し、ユーザの個人情報 $ID_k$ と鍵 $K_{k_1}$ を得る(ステップS2106)。

【0112】次に、この鍵 $K_{k_1}$ を用いて、鍵情報配信センタ2より受信した暗号文 $C_{k_1}$ ( $=E_{k_1}(E_{k_1}(K) \parallel ID_k)$ )を復号化して、ユーザの個人情報 $ID_k$ を得る(ステップS2107)。

【0113】それから、解除情報入手部112は、ステップS2106で暗号文 $C_{k_1}$ を復号化することで得たユーザの個人情報 $ID_k$ と、ステップS2107で暗号文 $C_{k_1}$ を復号化することで得たユーザの個人情報 $ID_k$ とを比較し、両者の一致を調べることで、ユーザ認証を行う(ステップS2108)。

【0114】ユーザ認証が成立しなかった場合(ステップS2109でNo)は、その旨を本ユーザ端末1に接続されているテレビ等に出力するなど所定のエラー処理を行い、それから、メモリ12上のワークエリアから鍵 $K_{k_1}$ 、 $K_{k_2}$ を除去して処理を終了する(ステップS2105)。

【0115】一方、ユーザ認証が成立した場合(ステップS2109でYes)は、鍵情報配信センタ2より受信した暗号文 $C_{k_1}$ を、主制御部114を介してメモリカード20に、当該メモリカード20に既に格納されている暗号文 $C_{k_1}$ と共に格納し(ステップS2110)、それから、メモリ12上のワークエリアから鍵 $K_{k_1}$ 、 $K_{k_2}$ を除去して処理を終了する(ステップS2111)。

【0116】次に、コンテンツ復号化処理について説明する。

【0117】図15は、本実施形態のコンテンツ復号化処理を説明するための図である。

【0118】ユーザ端末1において、コンテンツ復号化部113は、アプリ処理部115によるアプリケーションデータ412の暗号化部分へのアクセスを監視する(ステップS2301)。そして、アプリ処理部115がアプリケーションデータ412の暗号化部分へアクセスし、主制御部114が暗号化データを読み出した場合

には、これをフェッチする。

【0119】次に、コンテンツ復号化部113は、主制御部114を介して、メモリカード20から暗号文 $C_{k_1}$ ( $=E_{k_1}(E_{k_1}(E_{k_1}(K_{k_1}) \parallel ID_k)$ )を読み出すと共に、記憶媒体4から鍵情報 $CK_{k_1}$ 424aを読み出す。そして、この鍵情報 $CK_{k_1}$ を用いて暗号文 $C_{k_1}$ を復号化することにより、ユーザの個人情報 $ID_k$ を得る(ステップS2302)。

【0120】それから、コンテンツ復号化部113は、主制御部114を介してフラッシュメモリ13からユーザの個人情報 $ID_k$ を読み出して、これとステップS2302で得たユーザの個人情報 $ID_k$ とを比較し、両者の一致を調べることで、ユーザ認証を行う(ステップS2303)。

【0121】ユーザ認証が成立しなかった場合(ステップS2304でNo)は、ステップS2301でフェッチした暗号化データをアプリ処理部115に渡し、その後、ステップS2301に戻る。

【0122】一方、ユーザ認証が成立した場合(ステップS2304でYes)は、主制御部114を介して、記憶媒体4から鍵情報 $CK_{k_1}$ 424bを読み出す。そして、ステップS2302で暗号文 $C_{k_1}$ を復号化することにより得たデータ( $E_{k_1}(E_{k_1}(K_{k_1}) \parallel ID_k)$ )を、この鍵情報 $CK_{k_1}$ で復号化し、鍵 $K_{k_1}$ を得る(ステップS2306)。また、主制御部114を介して、メモリカード20から暗号文 $C_{k_1}$ ( $=E_{k_1}(E_{k_1}(K) \parallel ID_k)$ )を読み出し、これをステップS2306で得た鍵 $K_{k_1}$ を用いて復号化し、ユーザの個人情報 $ID_k$ を得る(ステップS2307)。

【0123】それから、コンテンツ復号化部113は、ステップS2306で暗号文 $C_{k_1}$ を復号化することで得たユーザの個人情報 $ID_k$ と、ステップS2306で暗号文 $C_{k_1}$ を復号化することで得たユーザの個人情報 $ID_k$ とを比較し、両者の一致を調べることで、ユーザ認証を行う(ステップS2307)。

【0124】ユーザ認証が成立しなかった場合(ステップS2308でNo)は、ステップS2301でフェッチした暗号化データをアプリ処理部115に渡し、その後、メモリ12上のワークエリアから鍵 $K_{k_1}$ を除去してステップS2301に戻る。

【0125】一方、ユーザ認証が成立した場合(ステップS2308でYes)は、主制御部114を介して、記憶媒体4から鍵情報 $CK_{k_1}$ 424cを読み出す。そして、ステップS2305での復号化により得たデータ( $E_{k_1}(K_{k_1})$ )を、この鍵情報 $CK_{k_1}$ で復号化し、鍵 $K_{k_1}$ を得る(ステップS2309)。次に、この鍵 $K_{k_1}$ を用いて、ステップS2306で暗号文 $C_{k_1}$ を復号化することで得たデータ( $E_{k_1}(K)$ )を復号化し、鍵 $K$ を得る(ステップS2310)。

【0126】それから、コンテンツ復号化部113は、



ステップS2301でフェッチした暗号化データを、ステップS2310で得た鍵Kを用いて復号化する（ステップS2311）。そして、復号化したデータをアプリ処理部115に渡した後、メモリ12上のワークエリアから鍵K、 $K_{11}$ 、 $K_{12}$ を除去して、ステップS2301に戻る。

【0127】以上、本発明の第2実施形態について説明した。

【0128】本実施形態によれば、解除情報配信センタ2において、ユーザ認証を行う前の時点で、鍵 $K_{11}$ 、 $K_{12}$ の内容が明らかにならず、また、ユーザ端末1において、ユーザ認証を行う前の時点で、鍵Kの内容が明らかにならないので、セキュリティが向上する。

【0129】なお、本実施形態では、3つの鍵情報 $G_K$ 、 $G_{K_1}$ 、 $G_{K_2}$ を用いて暗号文 $C_{1,1}$  ( $=E_{K_{11}}(E_{K_{12}}(E_{K_{11}}(K_{12}) \parallel ID_1))$ )を作成しているが、2つの鍵情報 $G_{K_1}$ 、 $G_{K_2}$ を用いて暗号文 $C_{1,1}$  ( $=E_{K_{11}}(E_{K_{12}}(K_{12} \parallel K_{11})) \parallel ID_1$ )を作成した場合でも、解除情報配信センタ2において、ユーザ認証を行う前の時点で鍵 $K_{11}$ 、 $K_{12}$ の内容が明らかにならないようにすることができる。

【0130】次に、本発明の第3実施形態について説明する。

【0131】上記の第1、2実施形態では、記憶媒体4に格納するコンテンツの利用制限を暗号化により実現している。これに対し、本実施形態では、記憶媒体4に格納するコンテンツの利用制限をアクセス制御により実現している。そして、当該コンテンツの所定部分へアクセス禁止を解除するための認証情報（解除情報）を、上記の第1、2実施形態と同様に、共通鍵暗号体系に従った当該コンテンツに固有の鍵情報を用いた、暗号通信により、解除情報配信センタ2からユーザ端末1へ送信するようにしている。

【0132】図16は、本実施形態で用いられる記憶媒体4のデータ構成図である。

【0133】ここで、図2に示す第1実施形態と同じ機能を有するものには、同じ符号を付している。図示するように、本実施形態では、アプリケーションデータ412は暗号化されていない。その代わり、アクセス制御プログラム425により、一部を除いて、アプリケーションプログラム411によるアプリケーションデータ412へのアクセスが禁止されている。認証情報AK426は、アプリケーションプログラム411によるアプリケーションデータ412のアクセス禁止領域へのアクセス禁止を解除するのに使用する情報であり、コンテンツ41に固有の情報である。

【0134】図17に、ユーザ端末1上に構築されるソフトウェア構成を示す。なお、ユーザ端末1のハードウェア構成は、第1実施形態のものと同様である。

【0135】本実施形態のユーザ端末1が図4に示す第1実施形態のものと異なる点は、コンテンツ復号化部1

13に代えてアクセス制御部116が設けられている点である。アクセス制御部116は、アクセス制御プログラム425により実現される。解除情報入手部112で入手した解除情報（認証情報）と記憶媒体4に記憶されている認証情報AK426とを用いて、アプリケーションデータ412のアクセス禁止領域へのアクセスを制御する。

【0136】なお、解除情報配信センタ2のハードウェア構成やソフトウェア構成も、基本的に第1実施形態のものと同様であるが、図18に示すように、管理テーブル212に、タイトル名212aおよびバージョン名212bにより特定されるコンテンツ41に固有の認証情報AK212hを格納している点が異なる。

【0137】次に、本実施形態の動作について説明する。

【0138】本実施形態の動作は、解除依頼生成処理、解除情報入手処理およびアクセス制御処理の3つに分けられる。このうち、解除依頼生成処理は図6に示す第1実施形態と同様である。また、解除情報入手処理も、暗号文 $C_{1,1}$ に含める解除情報が、解除依頼に含まれるコンテンツのタイトルおよびバージョンに対応する鍵K212dから認証情報AK212hに代わる点を除いて図7、図8に示すものと同じである。そこで、ここでは、アクセス制御処理についてのみ説明する。

【0139】図19は、本実施形態のアクセス制御処理を説明するための図である。

【0140】ユーザ端末1において、アクセス制御部116は、アプリ処理部115によるアプリケーションデータ412のアクセス禁止部分へのアクセスを監視する（ステップS3301）。そして、アプリ処理部115が、アプリケーションデータ412のアクセス禁止部分へのアクセスを主制御部114に依頼した場合には、これをフェッチする。

【0141】次に、アクセス処理部116は、主制御部114を介して、メモリカード20から暗号文 $C_{1,1}$ を読み出すと共に、記憶媒体4から鍵情報GK424を読み出す。そして、この鍵情報GKを用いて暗号文 $C_{1,1}$ を復号化することにより、鍵 $K_1$ とユーザの個人情報ID $_1$ を得る（ステップS3302）。

【0142】それから、アクセス処理部116は、主制御部114を介して、フラッシュメモリ13からユーザの個人情報ID $_1$ を読み出して、これとステップS3302で暗号文 $C_{1,1}$ を復号化することで得たユーザの個人情報ID $_1$ とを比較し、両者の一致を調べることで、ユーザ認証を行う（ステップS3303）。

【0143】ユーザ認証が成立しなかった場合（ステップS3304でNo）は、ステップS1301でフェッチした依頼を主制御部114に渡すことなく破棄し、その後、メモリ12上のワークエリアから鍵 $K_1$ を除去してステップS3301に戻る。

【0144】一方、ユーザ認証が成立した場合（ステップS3304でYes）は、主制御部114を介してメモリカード20から暗号文C<sub>1</sub>を読み出し、これをステップS3302で得た鍵K<sub>1</sub>を用いて復号化し、認証情報AKとユーザの個人情報ID<sub>1</sub>を得る（ステップS3305）。

【0145】それから、アクセス制御部116は、ステップS3302で暗号文C<sub>1</sub>を復号化することで得たユーザの個人情報ID<sub>1</sub>と、ステップS3305で暗号文C<sub>2</sub>を復号化することで得たユーザの個人情報ID<sub>2</sub>とを比較し、両者の一致を調べる。そして、両者が一致する場合は、主制御部114を介して記憶媒体4から認証情報AK426を読み出し、これと、ステップS3305で暗号文C<sub>2</sub>を復号化することで得た認証情報AKとの一致を調べる。これにより、アクセス禁止部分へのアクセスを許可するか否かの認証を行う（ステップS3306）。

【0146】認証が成立しなかった場合（ステップS3307でNo）は、ステップS3301でフェッチした依頼を主制御部114に渡すことなく破棄し、その後、メモリ12上のワークエリアから認証情報AK、鍵K<sub>1</sub>を除去して、ステップS3301に戻る。

【0147】一方、認証が成立した場合（ステップS3307でYes）は、ステップS3301でフェッチした依頼を主制御部114に渡し、アプリ処理部115によるアプリケーションデータ412のアクセス禁止部分へのアクセスを許可する（ステップS3308）。その後、メモリ12上のワークエリアから認証情報AK、鍵K<sub>1</sub>を除去して、ステップS3301に戻る。

【0148】以上、本発明の第3実施形態について説明した。

【0149】本実施形態も、上記の第1実施形態と同様の効果を有する。加えて、本実施形態では、コンテンツの復号化処理を行うことなく、コンテンツの利用を制限しているので、CPUにかかる負荷をより低減できる。

【0150】なお、本実施形態においても、上記の第1実施形態と同様の変形が可能である。また、上記の第2実施形態と同様に、解除情報配信センタ2において、ユーザ認証を行う前の時点で、鍵K<sub>1</sub>の内容が明らかにならないように、多重に暗号化を施して暗号文C<sub>1</sub>を作成すると共に、ユーザ端末1において、ユーザ認証を行う前の時点で、認証情報AKの内容が明らかにならないように、多重に暗号化を施して暗号文C<sub>2</sub>を作成するようにして、セキュリティを強化することもできる。

【0151】この場合、解除依頼生成処理は図12に示す第2実施形態と同様である。また、解除情報入手処理も、暗号文C<sub>1</sub>に含める解除情報が、解除依頼に含まれるコンテンツのタイトルおよびバージョンに対応する鍵K212dから認証情報AK212hに代わる点を除いて図13、図14に示すものと同じである。また、アクセス制御処理は、図19に示すアクセス制御処理におい

て、ステップS3302～ステップS3305に代えて図15に示すステップS2302～S2310（但し、鍵Kに代えて認証情報AKとする）を採用したものとなる。

【0152】次に、本発明の第4実施形態について説明する。

【0153】本実施形態では、上記の第1実施形態と同様、記憶媒体4に格納するコンテンツの利用制限を暗号化により実現している。但し、当該コンテンツの暗号化部分を復号するための復号鍵（解除情報）を、RSA暗号体系に従った当該コンテンツに固有の秘密鍵と公開鍵を用いた、暗号通信により、解除情報配信センタ2からユーザ端末1へ送信するようにしている。

【0154】まず、記憶媒体4のデータ構成について説明する。

【0155】図20は、本実施形態で用いられる記憶媒体4のデータ構成図である。ここで、図2に示す第1実施形態のものと同じものには同じ符号を付している。

【0156】図示するように、本実施形態の利用制限解除プログラム42は、解除情報入手プログラム427と、コンテンツ復号化プログラム423と、RSA暗号体系に従った、コンテンツ41に固有の公開鍵(n,e)429と、を有する。なお、ここでは、いわゆるバージョンの相違も異なるコンテンツとみなしている。

【0157】図21に、ユーザ端末1上に構築されるソフトウェア構成を示す。なお、ユーザ端末1のハードウェア構成は、第1実施形態のものと同様である。

【0158】本実施形態のユーザ端末1が図4に示す第1実施形態のものと異なる点は、鍵生成部111が省略されている点、および、解除情報入手部112に代えて解除情報入手部117が設けられている点である。解除情報入手部117は、解除情報入手プログラム427により実現され、記憶媒体4に格納されている公開鍵(n,e)429を用いて、解除情報配信センタ2より入手した暗号文を復号化し、コンテンツ復号化のための鍵K（解除情報）を入手する。

【0159】なお、解除情報配信センタ2のハードウェア構成やソフトウェア構成も、基本的に第1実施形態のものと同様であるが、図22に示すように、管理テーブル212に、タイトル名212aおよびバージョン名212bにより特定されるコンテンツ41に固有の秘密鍵(n,d)212i（当該コンテンツ41に固有の公開鍵(n,e)429と対の鍵）を格納している点が異なる。また、解除情報送信部211に代えて解除情報送信部214を設けた点が異なる。解除情報送信部214は、コンテンツ復号化のための鍵K（解除情報）を含む情報を、秘密鍵(n,d)212iで暗号化し、ユーザ端末1へ送信する。

【0160】次に、本実施形態の動作について説明する。

【0161】本実施形態の動作は、ユーザ端末1が、解除依頼を鍵情報配信センタ2に送信して、鍵情報配信センタ2から鍵K（解除情報）を入手する解除情報入手処理、および、入手した鍵Kを用いてコンテンツ41の暗号化部分を復号化するコンテンツ復号化処理の2つに分けられる。

【0162】まず、解除情報入手処理について説明する。

【0163】図23および図24は、本実施形態の解除情報入手処理を説明するための図であり、図23はユーザ端末1側での処理を、そして、図24は鍵情報配信センタ2側での処理を示している。

【0164】まず、ユーザ端末1において（図23参照）、主制御部114は、入力装置15を介してユーザより解除情報入手の指示を受け付けると、解除情報入手部117に指示を出す。これを受けて、解除情報入手部117は、主制御部114を介して、フラッシュメモリ13からユーザの個人情報ID<sub>u</sub>を読み出すと共に、記憶媒体4からコンテンツ41のタイトルおよびバージョン名を読み出す。そして、ユーザの個人情報ID<sub>u</sub>とコンテンツのタイトルおよびバージョン名とを含んだ解除依頼を作成し（ステップS4101）、解除情報配信センタ2に送信する（ステップS4102）。なお、ここで、個人情報ID<sub>u</sub>は、セキュリティ強化のため、例えば記憶媒体4に格納されている公開鍵(n,e)429で暗号化しておくようにしてもよい。

【0165】解除情報配信センタ2において（図24参照）、解除情報送信部214は、ユーザ端末1より解除依頼を受信すると（ステップS4201）、当該解除依頼に含まれているユーザの個人情報ID<sub>u</sub>を課金処理部213に渡す。なお、個人情報ID<sub>u</sub>が公開鍵(n,e)429で暗号化されている場合は、管理テーブル212に格納されている、当該解除依頼に含まれるコンテンツのタイトルおよびバージョン名に対応する秘密鍵(n,d)212i（これは当該コンテンツを格納する記憶媒体4の利用制限解除プログラム42に格納されている公開鍵(n,e)429と対の鍵である）で復号化してから、課金処理部213に渡す。

【0166】これを受けて、課金処理部213は、解除依頼を送信したユーザ端末1のユーザの認証を行う（ステップS4202）。例えば、解除情報送信部214より渡された解除依頼に含まれているユーザの個人情報ID<sub>u</sub>が正規のユーザとして記憶装置等に登録されているかを調べ、登録されているならば、ユーザ認証が成立したものとす。

【0167】ユーザ認証が成立しなかった場合（ステップS4203でNo）は、その旨を解除情報送信部214に知らせて、前記解除依頼を送信したユーザ端末1にエラー通知を送信する（ステップS4204）。

【0168】一方、ユーザ認証が成立した場合（ステッ

プS4203でYes）は、そのユーザの個人情報ID<sub>u</sub>により特定されるユーザに対して課金処理を行い（ステップS4205）、その旨を解除情報送信部214に知らせる。解除情報送信部214は、管理テーブル212から、受信した解除依頼に含まれているコンテンツのタイトルおよびバージョン名に対応する秘密鍵(n,d)212iと鍵K212dを読み出し、この鍵Kと前記ユーザの個人情報ID<sub>u</sub>とを繋げたデータ(K||ID<sub>u</sub>)を、秘密鍵(n,d)で暗号化して、暗号文C<sub>1</sub>（=(K||ID<sub>u</sub>)<sup>d</sup> mod n）を生成し（ステップS4206）、前記解除依頼を送信したユーザ端末1に送信する（ステップS4207）。

【0169】ユーザ端末1において（図23参照）、解除情報入手部117は、解除情報配信センタ2より情報を受信すると（ステップS4103）、それがエラー通知ならば（ステップS4104でNo）、その旨を本ユーザ端末1に接続されているテレビ等に出力するなど所定のエラー処理を行う（ステップS4105）。一方、暗号文C<sub>1</sub>ならば（ステップS4104でYes）、記憶媒体4から公開鍵(n,e)429を読み出す。そして、この公開鍵(n,e)を用いて暗号文C<sub>1</sub>を復号化し（C<sub>1</sub><sup>e</sup> mod n）、コンテンツ41復号化のための鍵Kとユーザの個人情報ID<sub>u</sub>を得る（ステップS4106）。

【0170】それから、解除情報入手部117は、ステップS4106で得たユーザの個人情報ID<sub>u</sub>を、フラッシュメモリ13より読み出したユーザの個人情報ID<sub>u</sub>と比較し、両者の一致を調べることで、ユーザ認証を行う（ステップS4107）。

【0171】ユーザ認証が成立しなかった場合（ステップS4108でNo）は、その旨を本ユーザ端末1に接続されているテレビ等に出力するなど所定のエラー処理を行うと共に、メモリ12上のワークエリアから復号結果を除去する（ステップS4105）。

【0172】一方、ユーザ認証が成立した場合（ステップS4108でYes）は、鍵情報配信センタ2より受信した暗号文C<sub>1</sub>を、主制御部114を介してメモリカード20に格納すると共に、メモリ12上のワークエリアから復号結果を除去する（ステップS4109）。

【0173】次に、コンテンツ復号化処理について説明する。

【0174】図25は、本実施形態のコンテンツ復号化処理を説明するための図である。

【0175】ユーザ端末1において、コンテンツ復号化部113は、アプリ処理部115によるアプリケーションデータ412の暗号化部分へのアクセスを監視する（ステップS4301）。そして、アプリ処理部115がアプリケーションデータ412の暗号化部分へアクセスし、主制御部114が暗号化データを読み出した場合には、これをフェッチする。

【0176】次に、コンテンツ復号化部113は、主制御部114を介して、メモリカード20から暗号文C<sub>2</sub>

10

20

30

40

50

を読み出すと共に、記憶媒体4から公開鍵 $(n, e)$  429  
を讀出す。そして、この公開鍵 $(n, e)$ を用いて暗号文 $C_{1,2}$   
を復号化することにより、鍵 $K$ とユーザの個人情報 $ID$   
を得る(ステップS4302)。

【0177】それから、コンテンツ復号化部113は、  
主制御部114を介してフラッシュメモリ13からユー  
ザの個人情報 $ID$ を読み出して、これとステップS43  
02で得たユーザの個人情報 $ID$ とを比較し、両者の一  
致を調べることで、ユーザ認証を行う(ステップS43  
03)。

【0178】ユーザ認証が成立しなかった場合(ステ  
ップS4304でNo)は、ステップS4301でフェッ  
チした暗号化データをアプリ処理部115に渡し、その  
後、メモリ12上のワークエリアから鍵 $K$ を除去して、  
ステップS4301に戻る。

【0179】一方、ユーザ認証が成立した場合(ステ  
ップS4304でYes)は、ステップS4301でフェ  
ッチした暗号化データを、ステップS4302で得た鍵  
 $K$ を用いて復号化する(ステップS4305)。そし  
て、復号化したデータをアプリ処理部115に渡した  
後、メモリ12上のワークエリアから鍵 $K$ を除去して  
(ステップS4306)、ステップS4301に戻る。

【0180】以上、本発明の第4実施形態について説明  
した。

【0181】本実施形態においても、上記の第1実施形  
態と同様、同じコンテンツ41であれば、当該コンテン  
ツ41と共に記録媒体4に記憶する公開鍵 $(n, e)$  429  
も同じものになるので、つまり、記憶媒体4毎に固有の  
情報を当該記憶媒体4に記憶させる必要がないので、当  
該記憶媒体4を例えばプレス等により大量生産するのに  
好適である。

【0182】加えて、本実施形態によれば、記憶媒体4  
に記憶される鍵を、RSA暗号体系に従った公開鍵 $(n, e)$   
としている。つまり、当該鍵からは解除情報配信セン  
タ2が保持する対の秘密鍵 $(n, d)$ を推測不可能な鍵とし  
ている。したがって、例えば不正な第3者が記憶媒体4  
の内容を解析して公開鍵 $(n, e)$ を入手したとしても、当  
該鍵からこれと対の秘密鍵 $(n, d)$ を求めることができな  
い以上、当該第3者が、前記公開鍵 $(n, e)$ で復号可能な  
解除情報(鍵 $K$ )を含む暗号文 $C_{1,2}$ を生成することはで  
きない。つまり、当該第3者が解除情報配信センタの運  
営者になりすまして、解除情報配信サービスの提供を行  
うのを防ぐことができる。

【0183】なお、上記の第4実施形態では、解除情報  
配信センタ2がユーザ端末1に送信する暗号文 $C_{1,2}$ を、  
コンテンツ復号化のための鍵 $K$ とユーザの個人情報 $ID$ と  
を繋げたデータ $(K || ID)$ を秘密鍵 $(n, d)$  212iで暗  
号化することで作成している。しかしながら、鍵 $K$ とユ  
ーザの個人情報 $ID$ にその他のデータを繋げたデータを  
秘密鍵 $(n, d)$ で暗号化することで、暗号文 $C_{1,2}$ を作成す

るようにしてもよい。例えば解除情報送信部214に乱  
数 $R$ を生成させ、鍵 $K$ とユーザの個人情報 $ID$ と乱数 $R$ を繋  
げたデータ $(K || ID || R)$ を、秘密鍵 $(n, d)$ で暗号化す  
ることで、暗号文 $C_{1,2}$ を $(K || ID || R)^d \bmod n$ 作成  
するようにしてもよい。このようにすれば、暗号文 $C_{1,2}$   
から鍵 $K$ が不正に解読される可能性をより低くできる。

【0184】また、上記の第4実施形態では、コンテン  
ツのタイトルのみならずバージョンが異なる場合でも、  
秘密鍵 $(n, d)$ と公開鍵 $(n, e)$ の対が異なるようにしてい  
るが、これに限定されない。例えば、コンテンツのタイ  
トルが同じであれば、バージョンにかかわらず同じ秘密  
鍵 $(n, d)$ と公開鍵 $(n, e)$ の対を用いるようにしてもかま  
わない。あるいは、同じコンテンツのタイトルに対し  
て、出荷時期等を考慮して、定期的に秘密鍵 $(n, d)$ と公  
開鍵 $(n, e)$ の対を変えるようにしてもよい。この場合、  
コンテンツ41に当該コンテンツ41の出荷時期がわか  
るような時期情報を入れておき、解除依頼にこの時期情  
報を含めて、ユーザ端末1から解除情報配信センタ2に  
送信する。そして、解除情報配信センタ2は、管理テー  
ブル212において、秘密鍵 $(n, d)$ をコンテンツのタイ  
トル名と時期情報とで管理することで、解除情報に含ま  
れるコンテンツのタイトル名および時期情報から秘密鍵  
 $(n, d)$ を特定することができる。

【0185】次に、本発明の第5実施形態について説明  
する。

【0186】上記の第4実施形態では、解除情報配信セ  
ンタ2は、ユーザ端末1に送信する暗号文 $C_{1,2}$ を、コンテ  
ンツ復号化のための鍵 $K$ とユーザの個人情報 $ID$ とを繋げ  
たデータ $(K || ID)$ を秘密鍵 $(n, d)$ を用いて暗号化する  
ことで作成している。このため、ユーザ端末1におい  
て、ユーザ認証を行う前の時点で、鍵 $K$ が取得されてしま  
う(図23のステップS4106、ステップS4107参照)。

【0187】そこで、本実施形態では、ユーザ端末1に  
おいて、ユーザ認証を行う前の時点で、鍵 $K$ の内容が明  
らかにならないように、多重に暗号化を施して暗号文 $C_{1,2}$   
を作成するようにして、セキュリティを強化してい  
る。

【0188】図26は、本実施形態で用いられる記憶媒  
体4のデータ構成図である。

【0189】ここで、図20に示す第4実施形態と同じ  
機能を有するものには、同じ符号を付している。図示  
するように、本実施形態では、利用制限解除プログラム4  
2に、RSA暗号体系に従った、コンテンツ41に固有  
の2つの公開鍵 $(n_1, e_1)$  429a、 $(n_2, e_2)$  429bを格  
納している。

【0190】なお、ユーザ端末1のハードウェア構成や  
ソフトウェア構成は、第4実施形態のものと同様であ  
る。また、解除情報配信センタ2のハードウェア構成や  
ソフトウェア構成も、基本的に第4実施形態のものと同

様であるが、図27に示すように、管理テーブル212に、タイトル名212aおよびバージョン名212bにより特定されるコンテンツ41に固有の、RSA暗号体系に従った2つの秘密鍵 $(n_1, d_1)$ 212j、 $(n_2, d_2)$ 212kを格納している点が異なる。

【0191】次に、本実施形態の動作について説明する。

【0192】本実施形態の動作も、上記の第4実施形態と同様に、解除情報入手処理およびコンテンツ復号化処理の2つに分けられる。

【0193】まず、解除情報入手処理について説明する。

【0194】図28および図29は、本実施形態の解除情報入手処理を説明するための図であり、図28はユーザ端末1側での処理を、そして、図29は鍵情報配信センタ2側での処理を示している。

【0195】まず、ユーザ端末1において(図28参照)、主制御部114は、入力装置15を介してユーザより解除情報入手の指示を受け付けると、解除情報入手部117に指示を出す。これを受けて、解除情報入手部117は、主制御部114を介して、フラッシュメモリ13からユーザの個人情報IDを読み出すと共に、記憶媒体4からコンテンツ41のタイトルおよびバージョン名を読み出す。そして、ユーザの個人情報IDとコンテンツのタイトルおよびバージョン名とを含んだ解除依頼を作成し(ステップS5101)、解除情報配信センタ2に送信する(ステップS5102)。なお、ここで、個人情報IDは、セキュリティ強化のため、例えば記憶媒体4に格納されている公開鍵 $(n_1, e_1)$ 429aで暗号化しておくようにしてもよい。

【0196】解除情報配信センタ2において(図29参照)、解除情報送信部214は、ユーザ端末1より解除依頼を受信すると(ステップS5201)、当該解除依頼に含まれているユーザの個人情報IDを課金処理部213に渡す。なお、個人情報IDが公開鍵 $(n_1, e_1)$ 429aで暗号化されている場合は、管理テーブル212に格納されている、当該解除依頼に含まれるコンテンツのタイトルおよびバージョン名に対応する秘密鍵 $(n_1, d_1)$ 212j(これは当該コンテンツを格納する記憶媒体4の利用制限解除プログラム42に格納されている公開鍵 $(n_1, e_1)$ 429aと対の鍵である)で復号化してから、課金処理部213に渡す。

【0197】これを受けて、課金処理部213は、解除依頼を送信したユーザ端末1のユーザの認証を行う(ステップS5202)。例えば、解除情報送信部214より渡された解除依頼に含まれているユーザの個人情報IDが正規のユーザとして記憶装置等に登録されているかを調べ、登録されているならば、ユーザ認証が成立したものとす。

【0198】ユーザ認証が成立しなかった場合(ステッ

プS5203でNo)は、その旨を解除情報送信部214に知らせて、前記解除依頼を送信したユーザ端末1にエラー通知を送信する(ステップS5204)。

【0199】一方、ユーザ認証が成立した場合(ステップS5203でYes)は、そのユーザの個人情報IDにより特定されるユーザに対して課金処理を行い(ステップS5205)、その旨を解除情報送信部214に知らせる。解除情報送信部214は、管理テーブル212から、解除依頼に含まれているコンテンツのタイトルおよびバージョン名に対応する秘密鍵 $(n_1, d_1)$ 212j、 $(n_2, d_2)$ 212jと、鍵K212dを讀出す。そして、この鍵Kを秘密鍵 $(n_2, d_2)$ で暗号化し、その暗号結果 $(K^{d_2} \bmod n_2)$ とユーザの個人情報IDとを繋げたデータ $((K^{d_2} \bmod n_2) \parallel ID_u)$ を、秘密鍵 $(n_1, d_1)$ でさらに暗号化して、暗号文 $C_{1,2} = ((K^{d_2} \bmod n_2) \parallel ID_u)^{d_1} \bmod n_1$ を生成し(ステップS5206)、前記解除依頼を送信したユーザ端末1に送信する(ステップS5207)。

【0200】ユーザ端末1において(図28参照)、解除情報入手部117は、解除情報配信センタ2より情報を受信すると(ステップS5103)、それがエラー通知ならば(ステップS5104でNo)、その旨を本ユーザ端末1に接続されているテレビ等に出力するなど所定のエラー処理を行う(ステップS5105)。一方、暗号文 $C_{1,2}$ ならば(ステップS5104でYes)、記憶媒体4から公開鍵 $(n_1, e_1)$ 429aを読み出す。そして、この公開鍵 $(n_1, e_1)$ を用いて暗号文 $C_{1,2}$ を復号化し $(=C_{1,2}^{e_1} \bmod n_1)$ 、ユーザの個人情報IDを得る(ステップS5106)。

【0201】それから、解除情報入手部117は、ステップS5106で得たユーザの個人情報IDを、フラッシュメモリ13より読み出したユーザの個人情報IDと比較し、両者の一致を調べることで、ユーザ認証を行う(ステップS5107)。

【0202】ユーザ認証が成立しなかった場合(ステップS5108でNo)は、その旨を本ユーザ端末1に接続されているテレビ等に出力するなど所定のエラー処理を行うと共に、メモリ12上のワークエリアから復号結果を除去する(ステップS5105)。

【0203】一方、ユーザ認証が成立した場合(ステップS5108でYes)は、鍵情報配信センタ2より受信した暗号文 $C_{1,2}$ を、主制御部114を介してメモリカード20に格納すると共に、メモリ12上のワークエリアから復号結果を除去する(ステップS5109)。

【0204】次に、コンテンツ復号化処理について説明する。

【0205】図30は、本実施形態のコンテンツ復号化処理を説明するための図である。

【0206】ユーザ端末1において、コンテンツ復号化部113は、アプリ処理部115によるアプリケーション

10

20

30

40

50

ンデータ412の暗号化部分へのアクセスを監視する（ステップS5301）。そして、アプリ処理部115がアプリケーションデータ412の暗号化部分へアクセスし、主制御部114が暗号化データを読み出した場合には、これをフェッチする。

【0207】次に、コンテンツ復号化部113は、主制御部114を介して、メモリカード20から暗号文 $C_1$ を読み出すと共に、記憶媒体4から公開鍵 $(n, e)$ 429aを読み出す。そして、この公開鍵 $(n, e)$ を用いて暗号文 $C_1$ を復号化することにより、ユーザの個人情報IDを得る（ステップS5302）。

【0208】それから、コンテンツ復号化部113は、主制御部114を介してフラッシュメモリ13からユーザの個人情報IDを読み出して、これとステップS5302で得たユーザの個人情報IDとを比較し、両者の一致を調べることで、ユーザ認証を行う（ステップS5303）。

【0209】ユーザ認証が成立しなかった場合（ステップS5304でNo）は、ステップS5301でフェッチした暗号化データをアプリ処理部115に渡し、ステップS5301に戻る。

【0210】一方、ユーザ認証が成立した場合（ステップS5304でYes）は、主制御部114を介して、記憶媒体4から公開鍵 $(n, e)$ 429bを読み出す。そして、この公開鍵 $(n, e)$ を用いて、ステップS5302にて暗号文 $C_1$ を復号化することで得たデータ $(K^e \bmod n)$ を復号化し、鍵Kを得る（ステップS5305）。そして、この鍵Kを用いて、ステップS5301でフェッチした暗号化データを復号化し（ステップS5306）、復号化したデータをアプリ処理部115に渡した後、メモリ12上のワークエリアから鍵Kを除去して（ステップS5307）、ステップS5301に戻る。

【0211】以上、本発明の第5実施形態について説明した。

【0212】本実施形態によれば、ユーザ端末1において、ユーザ認証を行う前の時点で、鍵Kの内容が明らかにならないので、セキュリティが向上する。

【0213】なお、上記の第4、5実施形態では、コンテンツ復号化のための鍵K（解除情報）を、RSA暗号を利用して解除情報配信センタ2からユーザ端末1へ送信するようにしているが、解除情報配信センタ2が保持する鍵（暗号鍵）が、ユーザ端末1が保持する前記鍵と対の鍵（復号鍵）からは推測不可能な非対称暗号を利用するものであれば、どのようなものであってもかまわない。

【0214】また、上記の第4、5実施形態では、記憶媒体4に格納するコンテンツの利用制限を暗号化により実現しているが、これらの実施形態を、上記の第3実施形態と同様に、記憶媒体4に格納するコンテンツの利用制限をアクセス制御により実現することも可能である。

つまり、上記の第3、4実施形態において、コンテンツ復号化のための鍵Kに代えて、コンテンツのアクセス禁止を解除するための認証情報AKを解除情報配信センタ2からユーザ端末1へ送信し、ユーザ端末1で、この受信した認証情報AKと記憶媒体4に記憶されている認証情報AKとの一致を調べることで、アクセス禁止を解除する可否か判断することも可能である。

【0215】以上、本発明の各実施形態について説明した。

【0216】本発明は、上記の各実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。

【0217】たとえば、上記の各実施形態において、利用制御解除プログラム42は、コンテンツ41のアプリケーションプログラム411の1部として組み込まれたものであってもかまわない。また、セキュリティ強化のため、利用制御解除プログラム42中の各プログラムが用いる暗号アルゴリズムは公開しない方が好ましい。

【0218】また、解除依頼のユーザ端末1から解除情報配信センタへの送信、および、解除情報の解除情報配信センタ2からユーザ端末1への送信は、上記の各実施形態のものに限定されるものではない。ネットワーク3上でのセキュリティが確保される方法によるものであれば、どのようなものであってもかまわない。

【0219】また、上記の第1、2、4および5実施形態では、コンテンツ41の1部を暗号化することでその利用を制限し、コンテンツ41の暗号化部分を復号化するための鍵Kを解除情報としている。また、上記の第3実施形態では、コンテンツ41の1部へのアクセスを禁止することでその利用を制限し、コンテンツ41のアクセス禁止部分へのアクセスを許可するための認証情報AKを解除情報としている。しかしながら、本発明はこれに限定されない。

【0220】本発明は、何らかの方法によりコンテンツの利用が制限されており、そのアクセス制限を解除するための情報が、ユーザ端末1による解除依頼に従い、解除情報配信センタ2からユーザ端末1へ送信されるものであればよい。

【0221】たとえば、図31に示すように、解除情報としてデジタル署名を用い、ユーザ端末1において、前記デジタル署名の検証を行い、その正当性が成立した場合にコンテンツ41の利用制限を解除するようにしてもよい。

【0222】なお、図31に示す例では、ユーザ端末1は、乱数、時刻情報、ユーザの個人情報ID、あるいは、コンテンツ41の識別情報、もしくは、これらの情報のうちの少なくとも2つの組み合わせでなる任意の情報Mを、解除依頼に含めて送信する（S6001）。これを受けて、解除情報配信センタ2は、コンテンツ41の利用制限の解除を許可する場合、例えばコンテンツ4



1 毎に固有の秘密鍵SKを用いて、前記解除情報に含まれる情報Mに対するデジタル署名sqnを生成し（S6002）、ユーザ端末1に送信する（S6003）。ユーザ端末1は、例えば記憶媒体4に格納されているコンテンツ41に固有の（秘密鍵SK対の）公開鍵PKを用いて、デジタル署名sqnを検証し（S6004）、当該署名の正当性が確認できた場合にのみ、メモリカード20等に格納する（S6005）。そして、ユーザ端末1は、コンテンツ41の利用制限部分にアクセスする都度、メモリカード20等からデジタル署名sqnを読み出して検証し、当該署名の正当性が確認できた場合にのみ、コンテンツ41の利用制限部分へのアクセスを許可する。

【0223】このようにした場合、ユーザ端末1は、デジタル署名sqnの正当性が確認できた場合にのみ、つまり、解除情報配信センタ2がコンテンツ41の利用制限の解除を許可していることが正しく確認できた場合にのみ、ユーザにコンテンツ41の利用制限部分の利用を許可することができる。

【0224】なお、解除情報配信センタ2における、コンテンツ41の利用制限の解除を許可するか否かの判断は、例えば図31に示す処理に先だて行われた、ユーザ認証処理や課金処理等での結果に基づいて行うようにしてもよい。あるいは、解除依頼中の情報Mにユーザの個人情報IDが含まれている場合、この個人情報IDが正規のユーザとして解除情報配信センタ2に登録されているか否かを調べることで行うようにしてもよい。また、ユーザ端末1側での処理を行うために必要なプログラム（解除依頼生成・送信のためのプログラムや署名検証のためのプログラムやコンテンツ41へのアクセスを制御するためのプログラム等）やデータ（コンテンツ41に固有の公開鍵PK等）は、上記の第1～第5実施形態と同様、コンテンツ41と共に記憶媒体4に格納しておくようにすればよい。

【0225】また、上記の各実施形態において、各種認証にユーザの個人情報IDを用いているが、当該情報の代わりに、ユーザ端末1のフラッシュメモリ13等に格納されているユーザ端末に固有の識別情報IDを用いるようにしても構わない。なお、上記の各実施形態において、ユーザ端末1にダウンロードされた解除情報（鍵Kや認証情報AK）はメモリカード20に格納されるが、上記の各実施形態では、ユーザ端末1のフラッシュメモリ13等に識別情報IDを格納し、この識別情報IDを用いて認証を行うことで、メモリカード20に格納された解除情報が不正にコピーされたり、あるいは、このメモリカード20が他の課金されていないユーザ端末1に装着されたりして、コンテンツが不正に使用可能となるのを防止している。

【0226】また、上記の各実施形態では、ユーザ端末1のフラッシュメモリ13に、予めOSを格納するようにしている。しかし、ユーザ端末1が記録媒体4からブ

ート可能に構成されている場合は、当該OSを記録媒体4に格納するようにしてもよい。なお、記録媒体4に格納されている各種プログラムが、OSプログラムを介さずに、直接、ユーザ端末1を各部を制御できる場合（いわゆるOSレス環境）、フラッシュメモリ13に予めOSプログラムを格納しておく必要はない。

【0227】また、上記の各実施形態では、ユーザ端末1での解除情報入手処理において、解除情報のメモリカード20への記録に先立ち認証を行っている。しかし、これは省略してもよい。この場合でも、ユーザ端末1でのコンテンツ復号化処理あるいはアクセス制御処理において認証を行っているので、コンテンツの不正な使用を制限できる。

【0228】

【発明の効果】以上説明したように、本発明によれば、ユーザに過度の負担をかけることなく、コンテンツの正規購入に先だてそのコンテンツを評価できるようにすることが可能となる。

【図面の簡単な説明】

【図1】本発明の各実施形態が適用されるコンテンツ利用制限解除システムの概略構成図である。

【図2】本発明の第1実施形態で用いられる記憶媒体4のデータ構成図である。

【図3】図1に示すユーザ端末1のハードウェア構成の一例を示す図である。

【図4】本発明の第1実施形態において、ユーザ端末1上に構築されるソフトウェア構成を示す図である。

【図5】本発明の第1実施形態において、解除情報配信センタ2上に構築されるソフトウェア構成を示す図である。

【図6】本発明の第1実施形態における解除依頼生成処理を説明するための図である。

【図7】本発明の第1実施形態における解除情報入手処理（ユーザ端末1側）を説明するための図である。

【図8】本発明の第1実施形態における解除情報入手処理（鍵情報配信センタ2側）を説明するための図である。

【図9】本発明の第1実施形態におけるコンテンツ復号化処理を説明するための図である。

【図10】本発明の第2実施形態で用いられる記憶媒体4のデータ構成図である。

【図11】本発明の第2実施形態において、解除情報配信センタ2上に構築されるソフトウェア構成を示す図である。

【図12】本発明の第2実施形態における解除依頼生成処理を説明するための図である。

【図13】本発明の第2実施形態における解除情報入手処理（ユーザ端末1側）を説明するための図である。

【図14】本発明の第2実施形態における解除情報入手処理（鍵情報配信センタ2側）を説明するための図であ



る。

【図15】本発明の第2実施形態のコンテンツ復号化処理を説明するための図である。

【図16】本発明の第3実施形態で用いられる記憶媒体4のデータ構成図である。

【図17】本発明の第3実施形態において、ユーザ端末1上に構築されるソフトウェア構成を示す図である。

【図18】本発明の第3実施形態において、解除情報配信センタ2上に構築されるソフトウェア構成を示す図である。

【図19】本発明の第3実施形態におけるアクセス制御処理を説明するための図である。

【図20】本発明の第4実施形態で用いられる記憶媒体4のデータ構成図である。

【図21】本発明の第4実施形態において、ユーザ端末1上に構築されるソフトウェア構成を示す図である。

【図22】本発明の第4実施形態において、解除情報配信センタ2上に構築されるソフトウェア構成を示す図である。

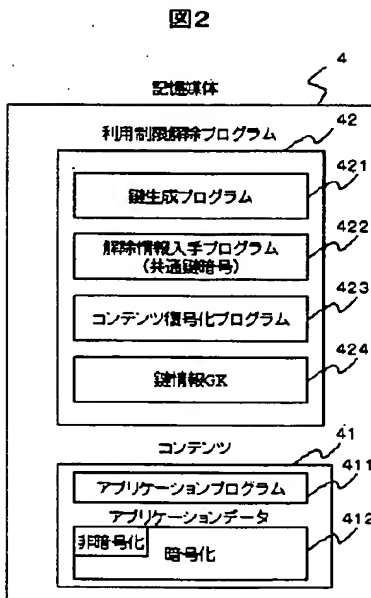
【図23】本発明の第4実施形態における解除情報入手処理（ユーザ端末1側）を説明するための図である。

【図24】本発明の第4実施形態における解除情報入手処理（鍵情報配信センタ2側）を説明するための図である。

【図25】本発明の第4実施形態のコンテンツ復号化処理を説明するための図である。

【図26】本発明の第5実施形態で用いられる記憶媒体\*

【図2】



\*4のデータ構成図である。

【図27】本発明の第5実施形態において、解除情報配信センタ2上に構築されるソフトウェア構成を示す図である。

【図28】本発明の第5実施形態における解除情報入手処理（ユーザ端末1側）を説明するための図である。

【図29】本発明の第5実施形態における解除情報入手処理（鍵情報配信センタ2側）を説明するための図である。

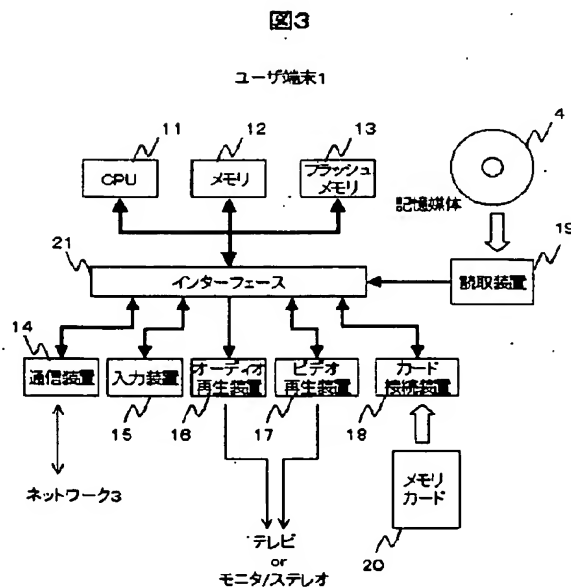
10 【図30】本発明の第5実施形態におけるコンテンツ復号化処理を説明するための図である。

【図31】本発明において、デジタル署名を利用して、コンテンツ41の利用制限を解除するようにした場合の処理の流れを説明するための図である。

【符号の説明】

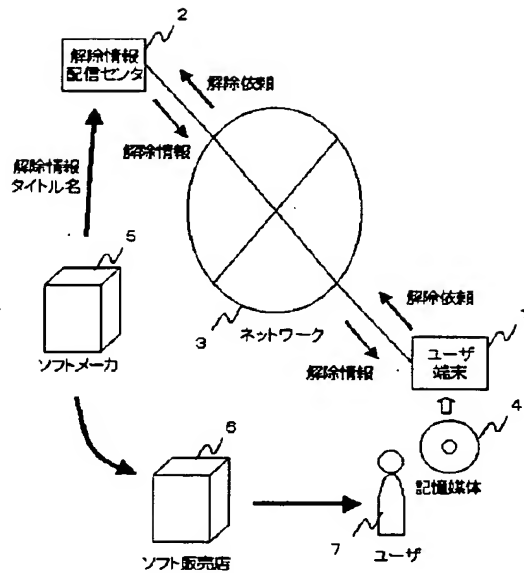
1…ユーザ端末、 2…解除情報配信センタ、 3…ネットワーク、 4…記憶媒体、 11…CPU、 12…メモリ、 13…フラッシュメモリ、 14…通信装置、 15…入力装置、 16…オーディオ再生装置、 17…ビデオ再生装置、 18…カード接続装置、 19…読取装置、 20…メモリカード、 21…インターフェース、 41…コンテンツ、 42…利用制御解除プログラム、 111…鍵生成部、 112, 117…解除情報入手部、 113…コンテンツ復号化部、 114…主制御部、 115…アプリ処理部、 116…アクセス制御部、 211, 214…解除情報送信部、 212…管理テーブル、 213…課金処理部

【図3】



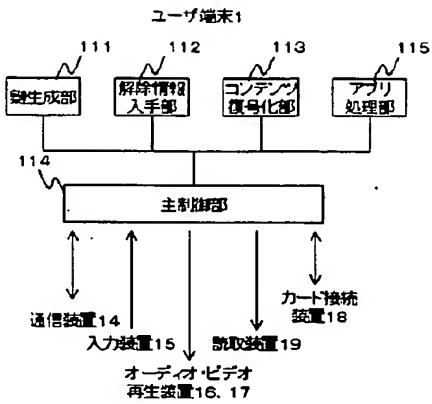
【図1】

図1



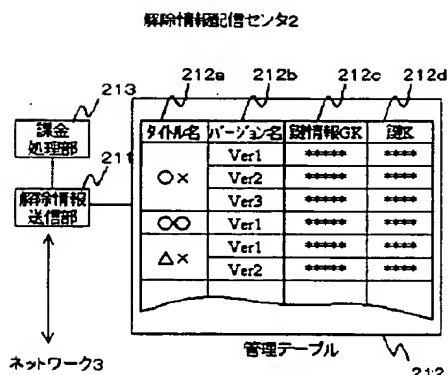
【図4】

図4



【図5】

図5

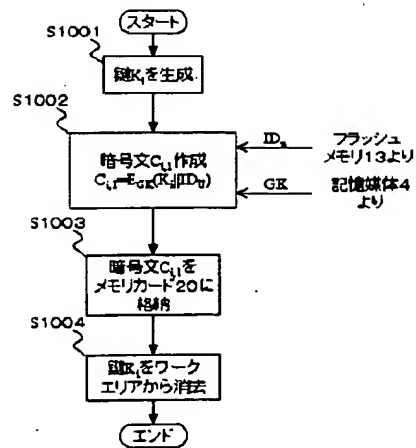


【図6】

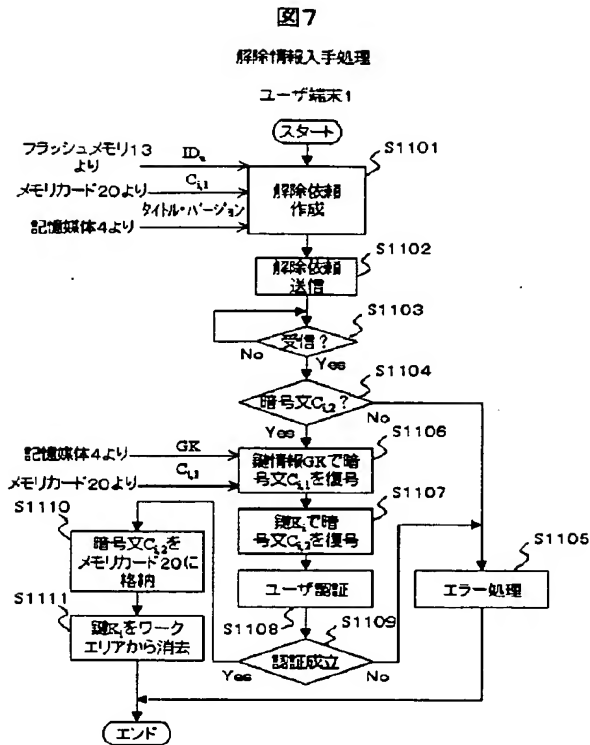
図6

解除依頼生成処理

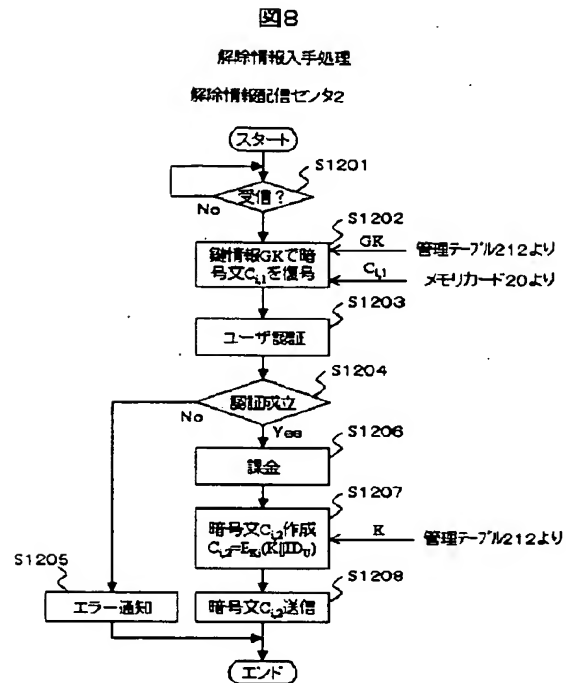
ユーザ端末1



【図7】



【図8】



【図9】

【図10】

図10

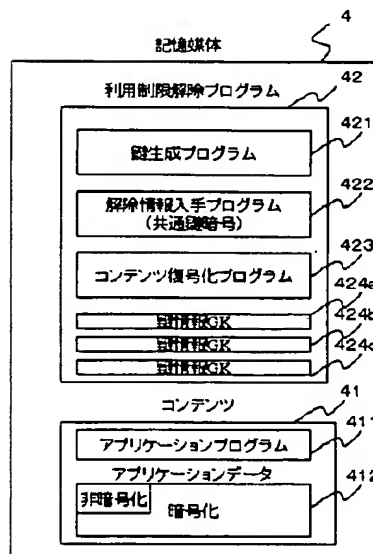
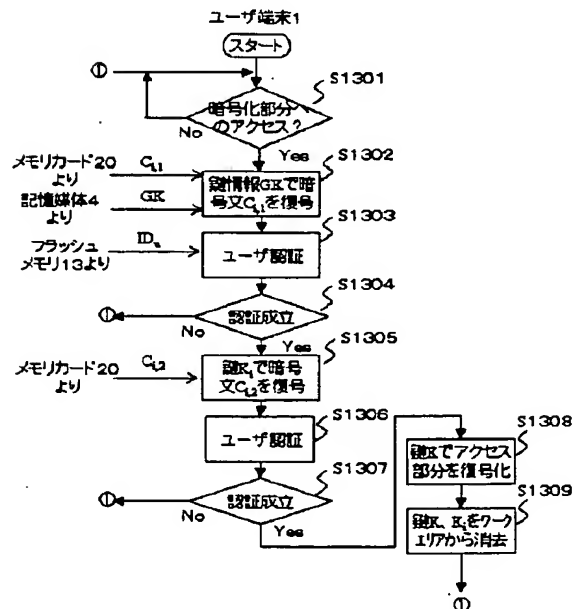
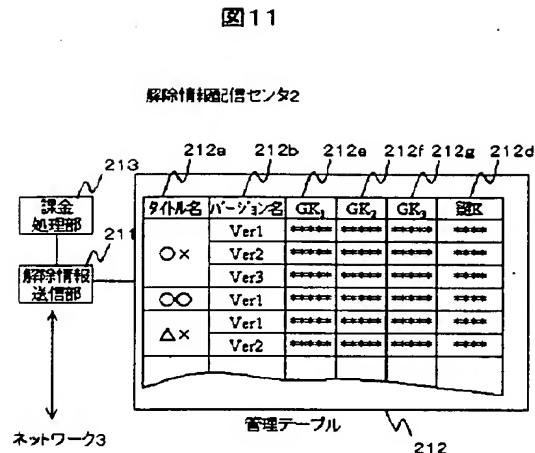


図9

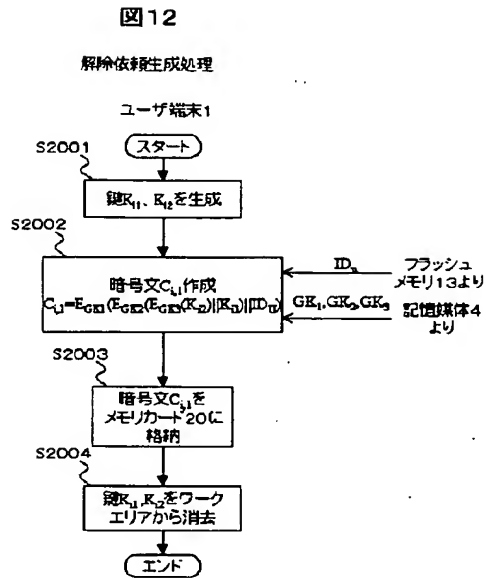
コンテンツ復号化処理



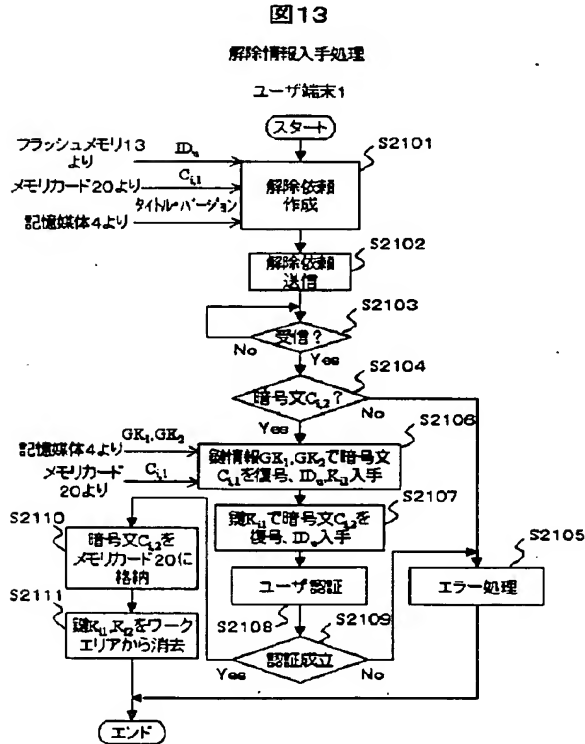
【図11】



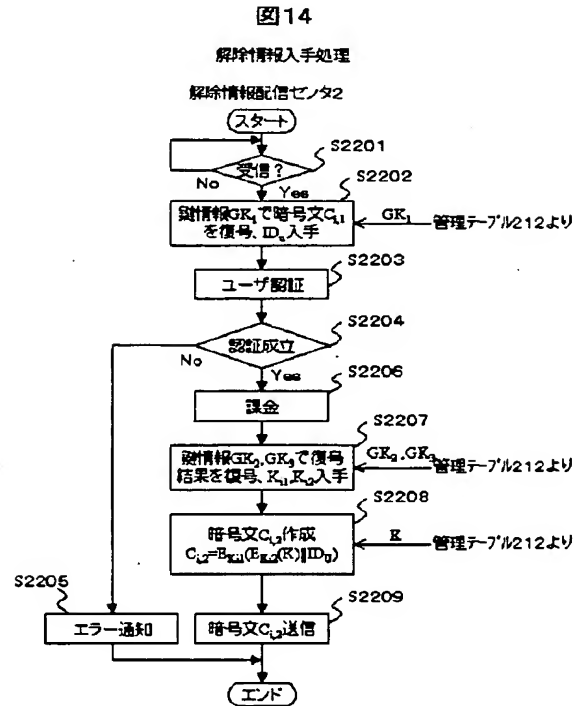
【図12】



【図13】



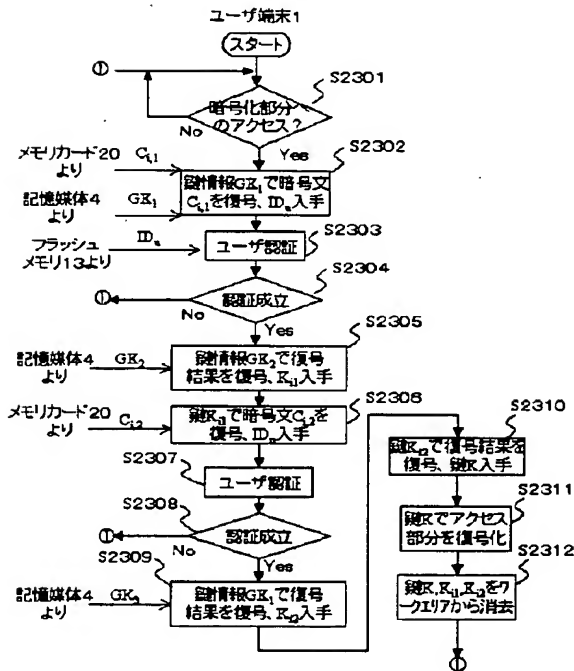
【図14】



【図15】

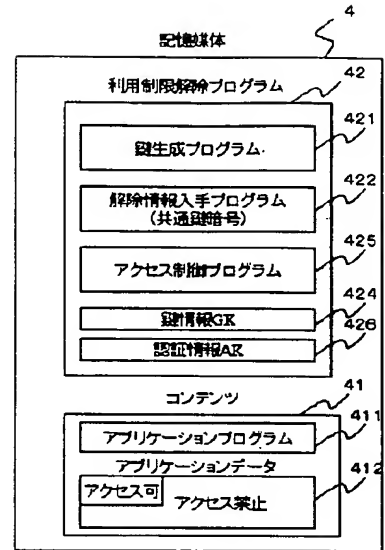
図15

コンテンツ復号化処理



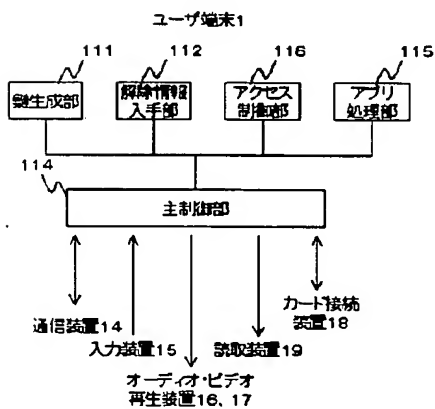
【図16】

図16



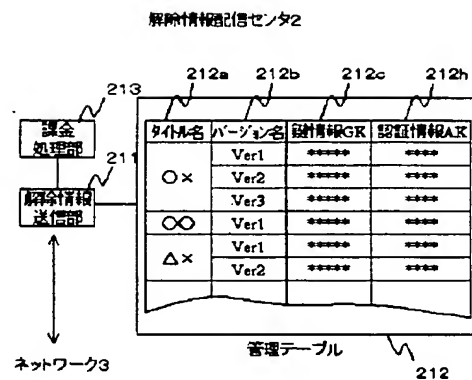
【図17】

図17

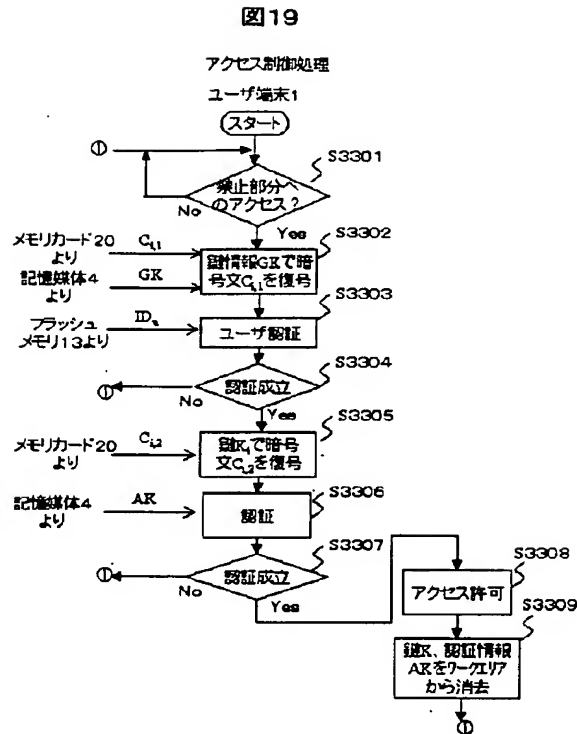


【図18】

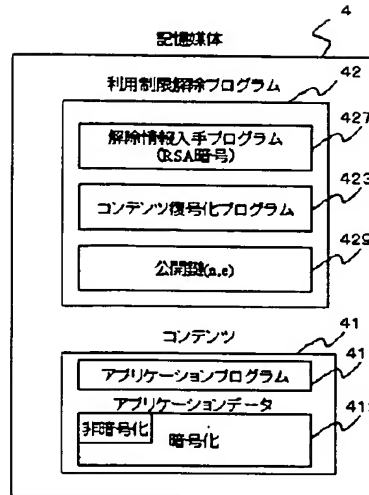
図18



【図19】

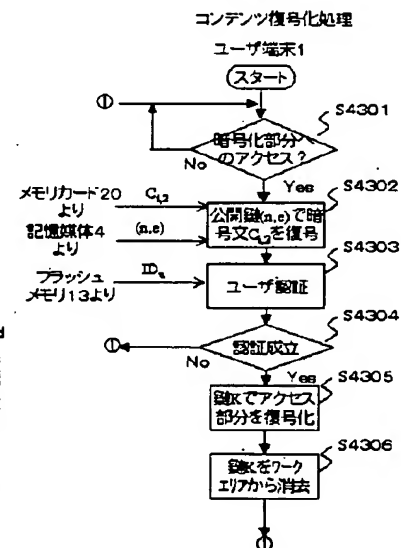


【図20】

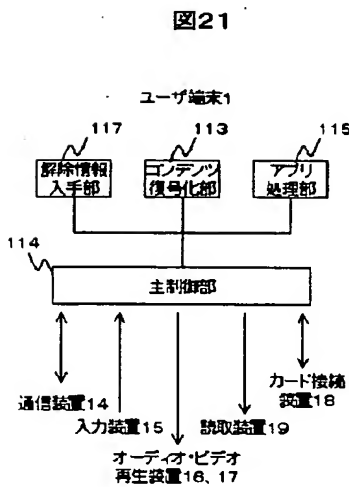


【図25】

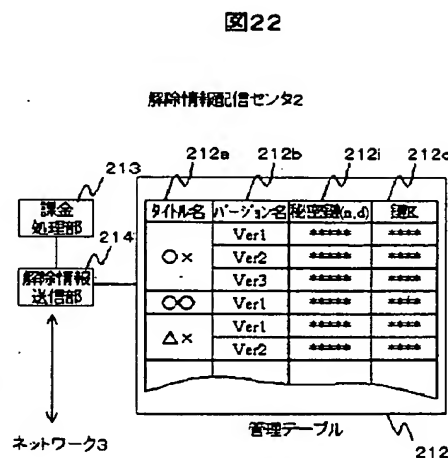
図25



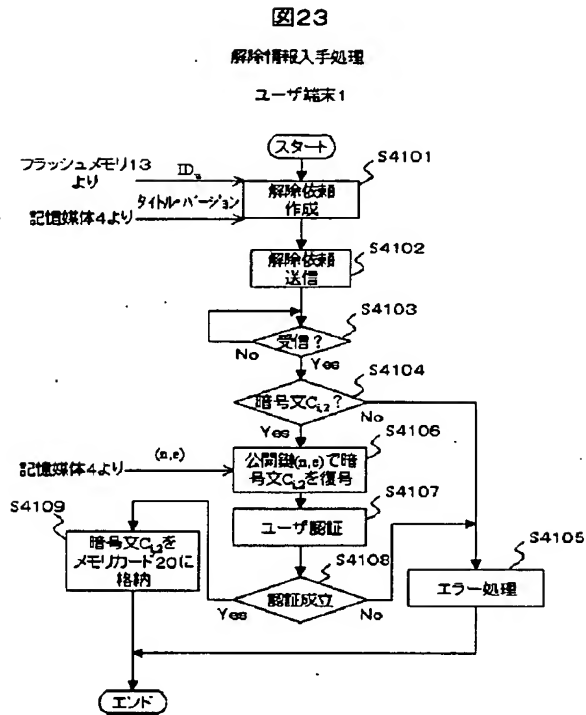
【図21】



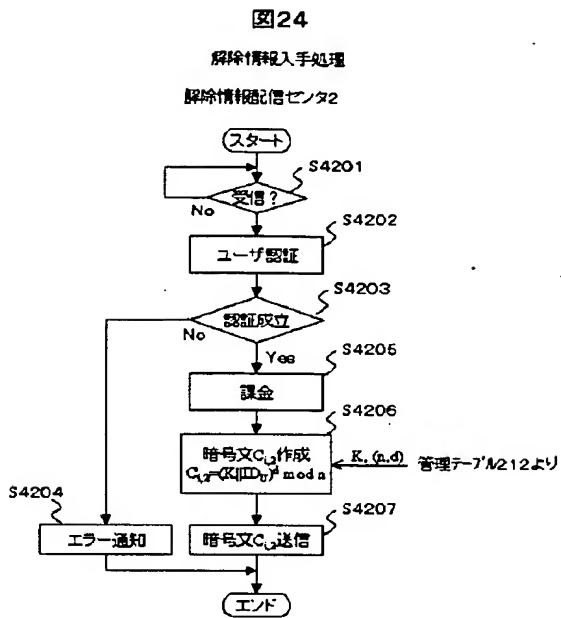
【図22】



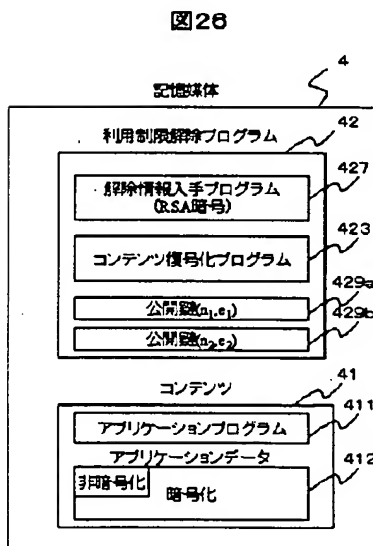
【図23】



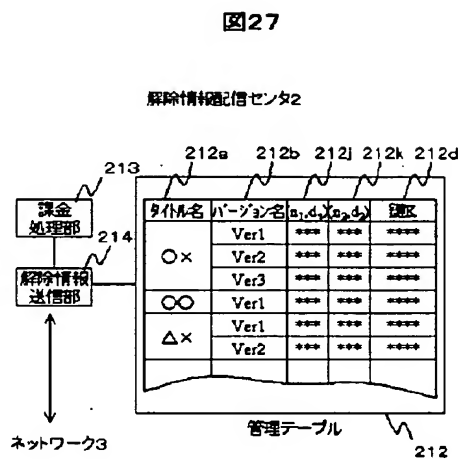
【図24】



【図26】

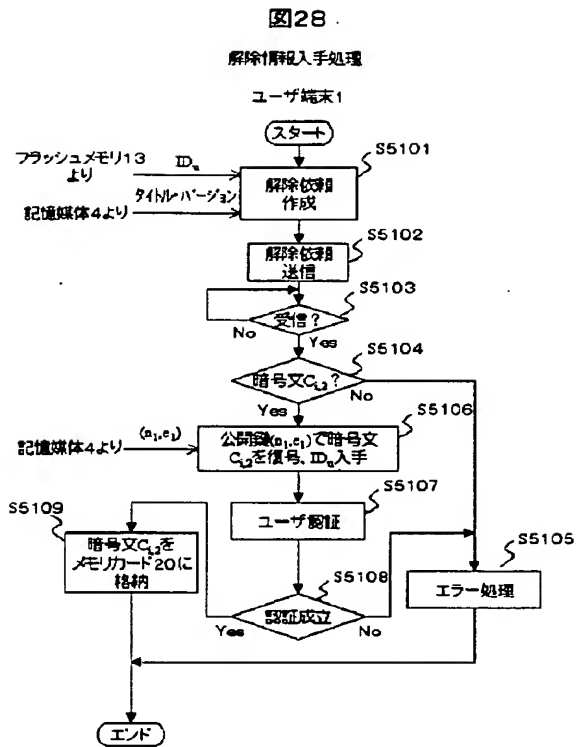


【図27】



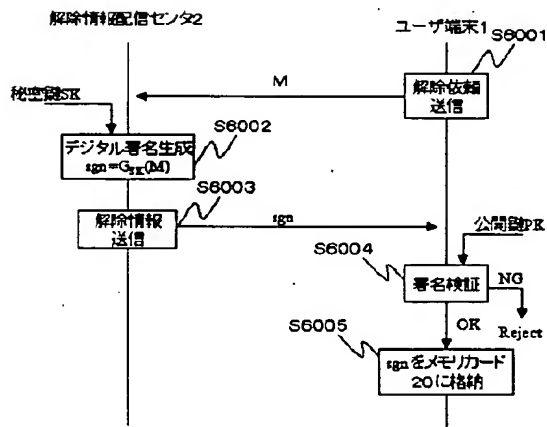


【図28】

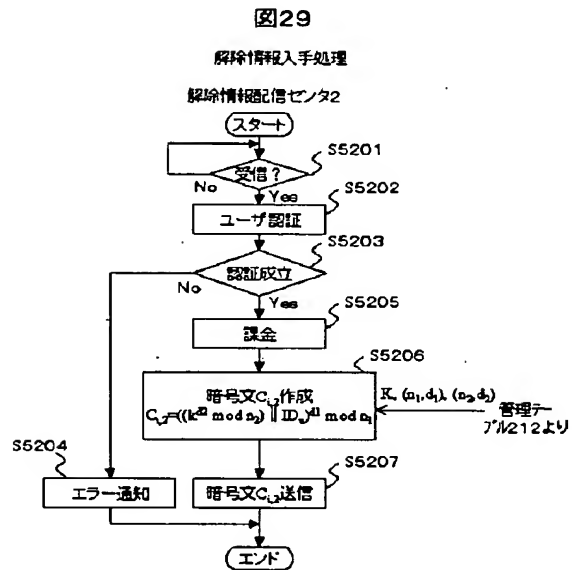


【図31】

図31

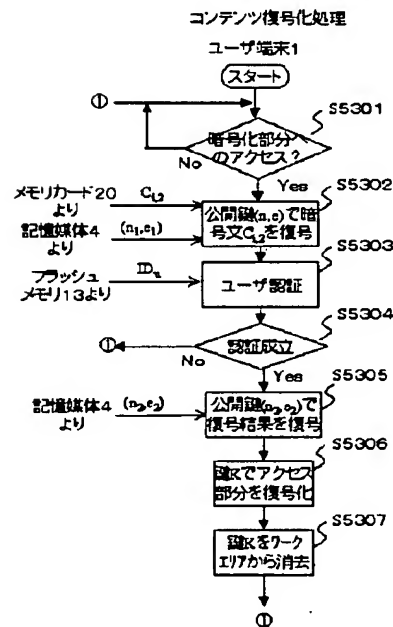


【図29】



【図30】

図30



## フロントページの続き

(51)Int.Cl. <sup>7</sup>	識別記号	F I	キーワード (参考)	
H 0 4 N	5/85	H 0 4 L	9/00	6 2 1 A
	5/91			6 7 3 A
	7/167			6 7 3 C
		H 0 4 N	5/91	P
			7/167	Z
(72)発明者	瀬戸 洋一	(72)発明者	山中 勇毅	
	神奈川県川崎市麻生区王禅寺1099番地 株		東京都大田区羽田1丁目2番12号 株式会	
	式会社日立製作所システム開発研究所内		社セガ・エンタープライゼス内	
(72)発明者	若林 隆	Fターム(参考)	5B085 AA08 AE29	
	神奈川県川崎市幸区鹿島田890番地 株式		5C052 AA02 AB04 AB05 CC20 DD04	
	会社日立製作所サービス事業部内		5C053 FA13 FA23 FA24 GB05 GB40	
(72)発明者	鉄井 俊明		JA30 LA14	
	東京都小平市上水本町五丁目20番1号 株		5C064 BA07 BB01 BB02 BC18 BD02	
	式会社日立製作所半導体グループ内		BD09 BD13	
			5J104 AA07 AA16 EA02 EA06 EA18	
			JA03 JA21 JA28 KA01 LA03	
			LA06 MA05 NA01 NA02 NA35	
			PA11	